

TOP SECRET

STUDY OF RUSSIAN

CRYPTOGRAPHIC SYSTEMS

By

Lieut. Waldemar Werther,
Cryptanalyst, 353rd Regiment, East
Luftwaffe SIS.

Note: This study is presented in the original German text for reasons explained in the Foreword.

J.G. S.

TOP SECRET

TOP SECRET

DIE GEBEDSCHRIFTEN DER SOWJETISCHEN FLIEGERTRUPPE UND IHRE

ENTZIFFERUNG

Von

Oberleutnant Waldemar Werther,
H-Regiment, Ost.

Vorbemerkung

I. Terminologie

II. Die Schluesselverfahren der sowjetischen Fliegertruppe

A. Einfuehrung

B. Das Charakteristische der sowjetischen Schluesselmethodik

C. Sowjetische Schluessel Systeme und -Formen

1. Allgemeines

- a) Einteilung der Verfahren nach dem Erscheinungsbild der Chi-Gruppen
- b) Sowjetische Schluesselbezeichnungen
- c) Die Lesart der Schluesselunterlage

2. Die sowjetische Schluesselunterlage

- a) Der einfache Caesar
- b) Der erweiterte Caesar
- c) Der mehrfach belegte Caesar
- d) Die Tafel
- e) Die Signaltafel
- f) Das Satzbuch
 - aa) Das lexikografische Satzbuch
 - bb) Das bedingt alfabetische Satzbuch

TOP SECRET

TOP SECRET

- cc) Das unalfabetische Satzbuch
 - dd) Das Satzbuch ohne Zahlenpositionen
 - ee) Das Satzbuch mit systematisch angeordneten Zahlenpositionen
 - ff) Das Satzbuch mit willkuerlich eingestreuten Zahlenpositionen
 - gg) Das Satzbuch mit eindeutigen Positionen
 - hh) Das Satzbuch mit mehrdeutigen Positionen
 - ii) Das Satzbuch mit einfacher Positionsbelegung
 - g) Das Formblatt
 - h) Der Kartenschluessel
 - i) Der Wetterschluessel
 - k) Die Uebungstafel
3. Die Ueberschluesselung
- a) Allgemeines
 - b) Der Ueberschluesselungswechsel
 - aa) Die langfristige Ueberschluesselung
 - bb) Die kurzfristige Ueberschluesselung
 - c) Die Kenngruppe
 - d) Das Ueberschluesselungssystem

III. Kurze geschichtliche Entwicklung der sowjetischen Fliegerverfahren und die Erfolge der deutschen Entzifferung

- A. Die Entwicklung bis zum Kriegsausbruch 1939
- 1. Die generelle 2Z-Tafel
 - 2. Der generelle 3Z-Fliegerschluessel
 - 3. Das generelle 4Z-Stabsverfahren
 - 4. Das generelle 5Z-Wumverfahren

TOP SECRET

TOP SECRET

- B. Die Besetzung Ostpolens im September 1939
 - 1. 2- und 3Z-Schlüssel
 - 2. Das 4Z-Stabsverfahren
 - 3. Das 5Z-Wurmverfahren
- C. Der finnische Winterkrieg
 - 1. 2-, 3- und 4Z-Verfahren
 - 2. Das 5Z-Wurmverfahren
- D. Der Ostkrieg 1941/45
 - 1. Die Erfolge der deutschen Entzifferung
 - 2. Die charakteristischen Veränderungen der sowjetischen Chiffrier-Methodik
 - a) Abschaffung der generellen Schlüsselverfahren - Einführung von Regionalverfahren
 - b) Verkürzung der Laufzeit der Verfahren
 - c) Komplizierung der Schlüsselunterlagen
 - d) Komplizierung der Ueberschlüsselungssysteme
 - e) Die Ähnlichkeit der Schlüssel Systeme
 - f) Abschaffung der generellen 2Z-Tafel und Umschulung auf Q-Gruppen
 - g) Individuelle Sprachueberschlüsselung
 - h) Verwendung von Blendern und Kontrollzahlen
 - i) Variierung der Lesart
 - k) Unterdrückung der Systematik
 - l) Das 5Z-Wurmverfahren
 - m) Das Auftreten von Versatzschlüsseln
 - n) Die Anwendung von Maschinenschlüsseln

TOP SECRET

TOP SECRET

IV. Organisation und Arbeitsweise der deutschen Entzifferung

- A. Kurzer geschichtlicher Rueckblick auf die organisatorische Entwicklung der deutschen Luftwaffen-Entzifferung Ost
- B. Gedanken zur organisatorischen Idealform
- C. Organisation und Arbeitsweise einer E-Abteilung
 - 1. Die E-Abteilung einer Auswerte-Kompanie
 - 2. Der Leiter der E-Abteilung (Chefentzifferer)
 - 3. Der Schichtdienst
 - 4. Der Schichtfuehrer
 - 5. Der Entzifferer
 - 6. Die Registratur
 - 7. Der "Bastler"
- D. Die Spruchbearbeitung
 - 1. Vorsortierung und Schluesselerkennungsdienst
 - 2. Die Entschluesselung
 - 3. Die Analyse
 - 4. Der Einbruch
 - 5. Die Systembearbeitung und Unterlagenerstellung
 - a) Das Aufgrundstellen der Schluesselunterlage
 - b) Die Erstellung des Uberschluesselungssystems
 - 6. Die Ausarbeitung
- E. Einige allgemeine Arbeitsgrundsaeetze
 - 1. Die Gemeinschaftsarbeit
 - 2. Die Raumfrage
 - 3. Die Statistik
 - 4. Die Verantwortlichkeit des Bearbeiters
 - 5. Die Spruchuebersetzung

TOP SECRET

TOP SECRET

6. Zum Personaleinsatz
7. Die Allgemeinverstaendlichkeit der persoenlichen Unterlagen
8. Einsatz weiblicher Arbeitskraefte
9. Militaerischer oder ziviler Einsatz?
- F. Die Hilfsmittel des Entzifferers
 1. Allgemeine Hilfsmittel
 2. Spezielle Hilfsmittel
 - a) Die Sprachstatistik
 - b) Das Brueckenverzeichnis
 - c) Das Idealsatzbuch
 - d) Das Statistikformular
 - e) Das Sprucharchiv
 3. Die Beuteauswertung
- G. Die Zusammenarbeit der E-Abteilung mit anderen Fachinstitutionen
 1. Die Zusammenarbeit mit den anderen Abteilungen der Auswerte-Kompanie
 - a) Die Zusammenarbeit mit dem Funker
 - b) Peil- und Betriebsauswertung
 - c) Inhalts- und Endauswertung
 2. Die Zusammenarbeit der E-Abteilung mit anderen Entzifferungsstellen
 - a) Regimentsentzifferung
 - b) Nachbarabteilungen des Regiments
 - c) E-Gruppen bei abgesetzten Kompanien der H-Abteilung
 3. Die Zusammenarbeit mit anderen Wehrmachtteilen und auslaendischen H-Diensten
 - a) Die Zusammenarbeit mit dem Heer
 - b) Die Kriegsmarine
 - c) Waffen-SS

TOP SECRET

TOP SECRET

- d) Der finnische H-Dienst
- e) Der ungarische H-Dienst

V. Der Entzifferer

- A. Geistige Voraussetzungen
- B. Die Auswahl des E-Personals
- C. Die Ausbildung des E-Personals
 - 1. Die laufende Ausbildung
 - 2. Der Lehrgang
 - 3. Das Lehrbuch

TOP SECRET

Oberleutnant Waldemar Werther.

DIE GEHEIMSCHRIFTEN DER SOWJETISCHEN FLIEGERGRUPPE UND IHR

ENTZIFFERUNG.

Vorbemerkung

In der folgenden Arbeit ist der Versuch unternommen worden, ein Bild ueber den Stand der Bearbeitung der sowjetischen Fliegersprueche durch die Entzifferung der deutschen Luftwaffe von der Gruendung dieses Dienstes (1936) bis zur Kapitulation (1945) zu geben.

Unter Beachtung des gegebenen Rahmens und infolge eines sehr lueckenhaften Unterlagensmaterials konnte dieses Bild sowohl fachlich als auch chronologisch nur in ganz groben Zuegen skizziert werden.

I. TERMINOLOGIE.

Wie bei jeder anderen wissenschaftlichen Disziplin ist auch bei der Entzifferung eine terminologische Festlegung aller Grundbegriffe unumgaenglich. Sie ist zum Verstaendnis der vorliegenden Arbeit besonders wichtig, weil die Eigenart des H-Dienstes die Existenz einer internationalen Terminologie ausschliesst. Die folgende Aufzaehlung erhebt keinen Anspruch auf Vollstaendigkeit, weil grundsatzlich nur die Ausdruecke aufgenommen worden sind, die in dieser Arbeit auftreten.

aufgrundstellung

Angleichung einer bereits relativ aufgestellten Schlusselfunterlage an das Original

"B"

heisst "Buchstabe"

Wigrammstatistik

Statistisierung eines Klar- oder Chi-Textes wobei immer zwei nebeneinanderliegende Klartextbuchstaben bzw. Chi-Gruppen als Einheit aufgefasst und erfasst werden.

TOP SECRET

Bereichsueberschliessung	<u>Ueberschliessungsform</u> , bei der eine <u>Satzbuchposition</u> durch eine Vielzahl von <u>Ueberschliessungszahlen</u> ausgedrueckt wird.
Blender	Ziffern, die - vollkommen willkuerlich gewaehlt, - den <u>Chi-Text</u> zur Irrefuehrung des Entzifferers veraendern; sie koennen ohne Schaden aus dem <u>Chi-Text</u> gestrichen werden.
Caesar	Einfachste Form eines <u>Ersatzverfahrens</u> , bei dem nur die Buchstaben des Alphabets durch eindeutige <u>Chi-Gruppen</u> ausgedrueckt werden.
<u>Chi-Gruppe</u>	Einheit eines <u>Chi-Textes</u> .
<u>Chi-Spruch</u>	<u>verschluesselter</u> Funk- oder Fernspruch.
<u>Chi-Text</u>	<u>Verschluesselter</u> Klar-Text.
"E"	heisst "Entzifferung".
E-Abteilung	Entzifferungs-Abteilung.
E-Mann	Entzifferer.
Einbruch	<u>Mitlesen</u> begrenzter <u>Chi-Spruech</u> - Stellen, wobei die gedeuteten <u>Chi-Gruppen</u> sich an anderer Stelle und in anderen Kombinationen im wesentlichen bestaetigen muessen.
Einsetzen	Das Bearbeiten von <u>Chi-Spruechen</u> nach bekannten <u>Schluessel-</u> und <u>Ueberschliessungsunterlagen</u> .
Element	Siehe <u>Position</u> .
Entcoden	Das Deuten von <u>Positionen</u> eines <u>Satzbuches</u> .
Entschluesseln	Siehe Einsetzen.
Entziffern	Das Bearbeiten von <u>Chi-Spruechen</u> , deren <u>Schluessel</u> und <u>Ueberschliessungsunterlagen</u> nicht bekannt sind.
Ersatzverfahren	<u>Schluesselverfahren</u> , bei dem Sprachelemente durch <u>E-Gruppen</u> (bzw. <u>B-Gruppen</u>) ersetzt werden.
Klartext	Normaler, allgemeinverstaendlicher Sprachtext das Resultat der <u>Entzifferung</u> bzw. <u>Entzifferung</u> bzw. <u>Entschluesseln</u> von <u>Chi-Spruechen</u> .

TOP SECRET

TOP SECRET

Kenngruppe	Siehe Schluesselgruppe.
Kontrollzahlen oder -Gruppen	Zahlen, die an sich keine Bedeutung haben und lediglich zur Bestaetigung anderer Zahlen dienen.
Lesart (einer Chi-Gruppe)	Die fuer ein <u>Verfahren</u> charakteristische Reihenfolge beim Herauslesen der einzelnen Ziffern aus der <u>Chi-Gruppe</u> bzw. <u>Schluesselunterlage</u> . Sie wird durch die ersten Buchstaben des Alphabets angezeigt, wobei A die erste, B die zweite, C die dritte, D die vierte und E die fuenfte Stelle der <u>Chi-Gruppe</u> bedeuten. ADBC heisst z.B.: "Lies von jeder <u>4-2-</u> (bzw. <u>4-B-</u>) <u>Gruppe</u> die einzelnen Stellen in der Reihenfolge 1-4-2-3 heraus". Die Lesart wird zuweilen auch durch kleine Buchstaben ausgedrueckt.
Mitlesen	Das Vermoegen, <u>Chi-Sprueche</u> des Gegners zu <u>entschluesseln</u> bzw. zu <u>entziffern</u> .
Original	Die urspruengliche Form einer Feind- <u>Schlueselunterlage</u> bzw. <u>-Ueberschluesselungsreihe</u>
Originalreihe	<u>Ueberschluesselungsreihe</u> mit den absoluten Zahlenwerten.
Position	Sprachelement einer <u>Schluesselunterlage</u> .
Quadrant	Horizontale Unterteilung einer <u>Satzbuchseite</u>
Raster	<u>Schluesselunterlage</u> in Form einer Schablone zur Verwurferung eines <u>Klar-Textes</u> .
Reduzieren	Das Auffinden eines Generalnenners fuer mehrere bzw. alle <u>Ueberschluesselungen</u> ein <u>Verfahrens</u> .
Satzbuch	Umfangreichere <u>Unterlage</u> eines <u>Ersatzverfahrens</u> . (Code).
Satzbuchelement	Siehe <u>Position</u> .
Schluessel	Unkompliziertes und im Format beschraenktes Gesamtsystem zur <u>Verschluesselung</u> .

TOP SECRET

TOP SECRET

Schlüsselgruppe	Gruppe im <u>Chi-Spruch</u> , die nicht zum Text gehört und lediglich auf die verwendete <u>Ueberschlüsselung</u> hinweist. (Indikator).
Schlüsselsicherheit	Grad der Sicherheit eines <u>Verfahrens</u> gegen <u>Entzifferungs</u> -Bestrebungen.
Schlüsselunterlage	Schriftlich festgelegte Unterlage zum <u>Ver-</u> <u>schlüsseln</u> (z.B. <u>Satsbuch</u>).
Schlüsselverfahren	Die Summe der Unterlagen eines <u>Verfahrens</u> , also <u>Schlüsselunterlage</u> und <u>Ueberschlüssel-</u> <u>system</u> .
Seite	Groebste vertikale Unterteilung eines <u>Satz-</u> <u>buches</u> .
Signalgruppe	Gruppe im <u>Chi-Spruch</u> , die nicht zum <u>Chi-Text</u> gehört und lediglich auf das verwendete <u>Ver-</u> <u>fahren</u> hinweist.
Spalte	Groebste vertikale Unterteilung einer <u>Tafel</u> .
Sprachstatistik	Auszählung und Ordnung von <u>Klartext</u> -elementen also Buchstaben, <u>Bigrammen</u> , usw.
Spruchstatistik	Auszählung und Ordnung der Gruppen eines <u>Chi-Textes</u> .
Statistikformular	Generierter Vordruck zur statistischen Erfas- sung von Sprach- oder Chi-Elementen.
Statistisierung	Auszählung von Chi- oder Sprachelementen und ihre gleichzeitige systematische Ordnung
Systemquadrat	Zusammenfassung von Ueberschlüsselungsreihen zu einem magischen Quadrat.
Systemtafel	Zusammenfassung von <u>Ueberschlüsselungsreihen</u>
Tafel	Kleinere <u>Schlüsselunterlage</u> eines <u>Erzatsver-</u> <u>fahrens</u> .
Tauschtafel	Behelf, nach dem <u>verschlüsselte Z-Gruppen</u> <u>ueberschlüsselt</u> werden koennen.
Trigrammstatistik	<u>Statistisierung</u> eines <u>Klar-</u> oder <u>Chi-Textes</u> , wobei immer d r e i nebeneinanderliegende <u>Klartext</u> -Buchstaben bzw. <u>Chi-Gruppen</u> als Einheit aufgefasst werden.

TOP SECRET

TOP SECRET

Trammel

In sich geschlossene Ueberschlüsselungsreihe die durch Veraenderung des Einsatzpunktes geaendert wird.

Ueberschlüsselung

Weitere Veraenderung des verschlüsselten Textes anhand besonderer Ueberschlüsselungsunterlagen zur Erhoehung der Schlüssel-sicherheit.

Ueberschlüsselungssuche

Bearbeitung von Chi-Material, bei dem nur die Verschlüsselung, d.h. die Schlüssel-
unterlage, nicht aber die verwendete Ueber-
schlüsselung bekannt ist.

Umschaltgruppe

Eindeutige Satzbuchposition, die andere mehr-
deutige Positionen des selben Satzbuches ein-
deutig bestimmt. Bedeutung der wichtigsten
Umschaltgruppen:

"Lesen Sie nur den Anfangsbuchstaben der
Position".

"Lesen Sie die ganze Position"
(das ganze Wort).

"Lesen Sie die linke (rechte) Seite der
Position".

"Lesen Sie die Zahlenbedeutung der Positi-

Verfahren

Siehe Schlüsselverfahren.

Versatzverfahren

Schlüsselverfahren, bei dem die Buchstaben
des Sprachtextes nicht ersetzt werden, sonder-
ihre Stellung im Gesamttext nach einem fest-
gelegten System veraendern, d.h. v e r -
s e t z t werden.

Verschlüsseln

Das Veraendern eines Klar-Textes anhand vor-
her festgelegter Unterlagen und vereinbarter
Arbeitsgaenge.

Wortcode

Satzbuchunterlage, deren Positionen nicht
aus Buchstaben und Silben, sondern nur aus
Woeatern bestehen. Das Herauslesen von
Buchstaben wird durch Umschaltgruppen er-
moeglicht.

Wuerfel

Einfachste Form eines Versatzverfahrens, bei
der die Klartextbuchstaben nach einem fest-
gelegten System verwuerfelt werden.

TOP SECRET

TOP SECRET

Wurmeberschlüsselung

Die Ueberschlüsselung von Z-Gruppen eines Chi-Textes mit einer ganz willkuerlich gewählten und praktisch unendlichen Zahlenreihe nach dem Prinzip der symbolischen Addition bzw. Subtraktion; hierbei wird das statistische Bild der Schlüsselunterlage restlos zerstört.

"Z"

Heisst "Zahl".

Zeile

Horizontale Unterteilung eines Quadranten oder einer Spalte, kleinste Einheit einer Schlüsselunterlage.

2Z-Gruppe

Zweistellige Zahlen-Chi-Gruppe.

3Z-Verfahren

Schlüsselverfahren, dessen Chi-Text aus 3Z-Gruppen besteht.

4B-Gruppe

Vierstellige Buchstaben-Chi-Gruppe.

5Z-Gruppe

Fuenfstellige Zahlen-Chi-Gruppe.

TOP SECRET

TOP SECRET

II. DIE SCHLUESSELVERFAHREN DER SOWJETISCHEN FLIEGERTRUPPE.

A. Einfuehrung.

Bis 1940 etwa kann man von sowjetischen Fliegerschlüsseln kaum sprechen, weil die organisatorische Unterstellung unter das Heer einen Gebrauch von eigenen Schlüsselmitteln garnicht notwendig machte. In der Regel war nur ein kleines Satzbuch fuer den Boden-Bord-Verkehr vorhanden, alle wichtigen Sprueche wurden aber nach dem allgemeinen 4-Z-Verfahren der Roten Armee verschlüsselt.

Eine vergleichende Betrachtung der Verfahren aller Teile der bewaffneten Macht der Sowjet-Union laesst erkennen, dass die Verfahren der einzelnen Wehrmachtteile sich in den Grundprinzipien nicht wesentlich voneinander unterscheiden. Die in der Folge getroffenen Feststellungen gelten zwar nur fuer die Fliegertruppe, sind aber **b e d i n g t** auch fuer die anderen Wehrmachtteile (Heer, Marine, NKWD und Partisanen) zutreffend.

B. Das Charakteristische der sowjetischen Schlüsselmethodik.

Das allgemein Charakteristische der sowjetischen Schlüsselmethoden kann durch folgende vier Punkte umrissen werden:

1. Die Sowjets verwenden fast ausschliesslich Zahlenschlüssel, also Eratzverfahren. Die wichtigste Schlüsselanterlage ist das Satzbuch. Demnach ist der sowjetische Funker auch nur auf das Arbeiten mit Zahlensymbolen spezialisiert.

2. Bemerkenswert ist der ausgesprochene und vielfach unmaetze Hang zu systematischen Konstruktionen sowohl bei der Erstellung der Schlüsselanunterlagen als auch der Ueberschlüsselungssysteme. Dabei handelt es sich einesteils

TOP SECRET

TOP SECRET

gewiss um eine spielerische Freude an der Systematik, andererseits kann aber daraus einwandfrei eine strafliche Bequemlichkeit und Sorglosigkeit der Ersteller neuer Verfahren gefolgert werden.

Auf Grund dieser Eigenart konnte manches Verfahren leichter gelöst und manche Ueberschlüsselung sogar im voraus rekonstruiert werden. In den letzten Jahren wurde diese Systematik anscheinend bewusst unterdrückt.

3. Die Geheimhaltung beim Chiffrierdienst der Sowjets ist sehr streng, das Schlüsselpersonal besteht ausschliesslich aus besonders ausgesuchten und ausgebildeten Offizieren. Trotzdem ist das allgemeine Niveau nicht hoch, die Zahl der auftretenden groben orthografischen Fehler z.B. ist sehr gross.

Infolge dieser Geheimhaltung ist es deshalb immer sehr schwer gewesen, brauchbare Nachrichten ueber das sowjetische Chiffrierwesen zu erhalten. Bei allen Gefangenenerhebungen stellte sich immer wieder heraus, dass auch der ueberdurchschnittlich intellegente sowjetische Offizier ueber den interessierenden Komplex nichts auszusagen wusste.

Andererseits hat die strenge Geheimhaltung zweifellos zu einer Ueberschaetzung der Schlüsselsicherheit der eigenen Verfahren gefuehrt.

Alle grundsatzlichen Schlüsselanweisungen sehen vor, dass alle Verfahren nicht nur fuer den Telegrafie- sondern auch fuer den Telefonie-Verkehr (Draht und drahtlos) Gueltigkeit haben. Leider war der deutsche Luftwaffen-H-Dienst nicht in der Lage, Drahtgespraeche der sowjetischen Fliegertruppe abzuhoeren.

4. Die Schlüsseldisziplin ist gering. Allgemein verbindliche Regeln, etwa fuer die Behandlung der Eigennamen, Satzzeichen oder Zahlen bei der Verschlüsselung

TOP SECRET

TOP SECRET

sind nicht vorhanden. Diese Grundsatzlosigkeit bedeutet fuer den Entzifferer eine Erschwerung seiner Arbeit, denn es gibt keine allgemein gueltigen Voraussetzungen; der Spruchaufbau ist nicht stereotyp, jeder Spruch kann demnach Ueberraschungen bringen.

Trots wiederholter und sehr strenger Verbote der hoeheren Fuehrung sind Schluesselangaben, -Anweisungen und -Bezeichnungen in Funkspruechen gebracht worden, manchmal sogar im Klartext. Durch diese Inkorrekttheiten im Funkverkehr konnte im Laufe der letzten Jahre die Bearbeitung einer Reihe von Verfahren wesentlich beschleunigt werden.

Eine spezifizierte Charakterisierung der sowjetischen Schluesselmethode nach der durch die Erfahrungen des Winterkrieges 1939/40 ausgelocsten Reorganisation auf diesem Gebiet befindet sich unter III. D. 2 auf Seite 23.

C. Sowjetische Schluesselsysteme und -Formen

1. Allgemeines

a) Einteilung der Verfahren nach dem Erscheinungsbild der Chi-Gruppen:

Nach der aeusseren Beschaffenheit der Gruppen eines Chi-Textes unterscheidet man 2-, 3-, 4-, 5-Z-Verfahren, 5-B-Verfahren und Texte mit gem. Gruppen (gemischt). Waehrend alle Z-Verfahren grundsatzlich nur Erstsatzsysteme sein koennen ist bei den B-Verfahren sowohl ein Erstsatz-(Maschinen-) als auch ein Versatzverfahren (Wuerfel, Raster) moeglich. Bei den Spruechen mit gem. Gruppen handelt es sich entweder um besondere Formblattsprueche oder aber um Uebungstexte.

Diese Einteilung hat sich aus organisatorischen Gruenden, insbesondere im Berichtswesen der anderen Fachabteilungen des H-Dienstes als zweckmaessig erwiesen.

TOP SECRET

TOP SECRET

von entsifferungstechnischen Standpunkt aus aber ist diese Unterteilung ziemlich nichtssagend. Denn sie deutet nicht ohne weiteres auf die Schwierigkeit eines Verfahrens hin, wenngleich die Erhöhung der Stellenzahl der Chi-Gruppe sowohl die Möglichkeit fuer die Vergrößerung der Schlüssellunterlage als auch fuer eine Erhöhung der Ueberschlüsselungsvariationen in sich schliessen kann - falls nicht die Anwendung von Blendern oder Kontrollzahlen diese Möglichkeit von vorn herein ausschliesst. Auch eine tatsächlich vorliegende Erweiterung der Unterlage sagt ueber die Schwierigkeit eines Verfahrens immer noch nichts Definitives aus: Ein kompliziert ueberschlüsseltes, unsystematisches 3Z-Satzbuch bereitet der Entzifferung mehr Schwierigkeiten als etwa ein lexikografisches und primitiv ueberschlüsseltes 4Z-Satzbuch. Es ist auch nicht angebracht, von der Schlüsselsicherheit des Verfahrens auf die auswertemaessige Wichtigkeit der danach verschlüsselten Spruchinhalte schliessen zu wollen. Zum allgemeinen Erstaunen hat sich z.B. beim Mitlesen der wurm ueberschlüsselten 5Z-Sprueche in den ersten Jahren des Ostfeldzuges herausgestellt, dass in diesen ueberaus kompliziert verschlüsselten Spruechen auch der hoeheren Staabe weniger Auswertbares gestanden hat als in den verhaeltnismaessig einfach mitzulesenden Spruechen irgendwelcher Flieger-Bodenbezirke.

b) Sowjetische Schlüssellbezeichnungen.

Bei einem Teil der rekonstruierten Verfahren konnte die sowjetische Originalbezeichnung festgestellt werden. Die meisten Deutungen liessen sich nach mitgelesenen Chi-Spruechen mit Schlüssellbezeichnungen und -Angaben vornehmen. Ein sehr geringer Teil dieser Deutungen ist auf Beuteunterlagen (Satzbuecher, Ueberschlüsselungsblocks, Befehle der Nachrichtenfuhrer mit Schlüssellanweisungen usw.) und Gefangenaussagen zurueckzufuehren.

TOP SECRET

TOP SECRET

Die Original-Schlüsselbezeichnungen setzen sich oft aus einer Abkürzung und der Jahreszahl der Einfuehrung dieses Schlüssels oder einer Ordnungszahl zusammen. Z.B.:

"pt 39" = peregowornaja tabliza 1939 = Sprechtafel 1939
"okk 5" = obschtschewojkowskij komandirskij kod nr. 5
= allgemeiner Kommandeur-Code Nr. 5.

Zuweilen hat der Schlüssel den Namen des Einheitsfuehrers, vielleicht auch den des Erstellers der Schlüsselunterlage, erhalten (z.B. "kod Rubin"). Manchmal wird das Verfahren mit einem Wort, das gleichzeitig die Signalgruppe dieses Verfahrens ist, bezeichnet (z.B. "oka" "karasj").

o) Die Lesart der Schlüsselunterlage.

Abgesehen von einigen umfangreichen Satzbuechern koennen die Positionen in den Unte lagen nicht vonvornherein durch Zahlengruppen ausgedrueckt bzw. herausgelesen werden. Dieser Arbeitsgang wird erst durch die Anlegung der entsprechenden Ueberschlüsselungsreihen moeglich gemacht.

Dabei ist die Wahl der Lesart wichtig. Je "unnatuerlicher" sie im Bezug auf den Aufbau der Schlüsselunterlage gewaehlt wird, desto schwieriger gestaltet sich fuer den Entzifferer die analytische Vorarbeit zur Rekonstruktion der Schlüsselunterlage.

2. Die sowjetische Schlüsselunterlage.

a) Der einfache Caesar

Es handelt sich meist um wilde Schlüsselunterlagen der Funker an der Taste zur Abwicklung des Verstaendigungsverkehrs neben dem Gebrauch der Q-Grup-

TOP SECRET

TOP SECRET

pen oder um Notchlüssel. Durch Blender und Kontrollzahlen wird vergeblich versucht, den ursprünglichen 2-Z-Charakter dieser Schlüssel zu verwischen.

Eine Ueberschlüsselung findet in der Regel nicht statt. Die Schlüsselsicherheit ist sehr gering, beim systematischen Aufbau des Caesars wird sie gleich Null.

b) Der erweiterte Caesar.

Der einfache Caesar wird durch Zahlen, Satzzeichen und zuweilen auch durch einige Bigramme und Silben bzw. Kurzwoerter ergaenzt.

Ansonsten gilt das unter a) Gesagte.

c) Der mehrfach belegte Caesar.

Durch die Zerstoerung des charakteristischen Bildes einer Buchstabenstatistik wird die Schlüsselsicherheit groesser. Im uebrigen gelten aber ebenfalls die Ausfuehrungen unter a).

d) Die Tafel. (russisch: "pt" = peregowornaja tabliza)

Bei diesen Tafeln handelt es sich meist um eine Schlüsselunterlage mit 10 x 10 Feldern. Die einzelnen Zeilen sind in der Regel zweideutig, die Eindeutigkeit des Chi-Textes wird durch Umschaltgruppen garantiert. In der Tafel befindet sich ein einfacher oder mehrfach belegter Caesar.

Die klar umrissene Form der Tafel ermoeoglicht die Anlegung einer Ueberschlüsselung. Dadurch kann die Tafel eine Schlüsselunterlage fuer laengere Zeit werden.

In den ersten Kriegsjahren noch wurden solche Tafeln als generelle Schlüsselunterlagen fuer den Panker an der Taste laufend verwendet, sind aber nun-

TOP SECRET

TOP SECRET

mehr vollkommen verschwunden und durch Q-Gruppen ersetzt worden. Die Schlüsselsicherheit ist nicht sehr gross, doch stoesst die vollstaendige Rekonstruktion insofern auf Schwierigkeiten, als die meisten Wortpositionen und Saetze im Chitext kaum auftauchen und aus diesem Grunde auch nicht gedeutet werden koennen.

e) Die Signaltafel (= "tablisa rediosignalow")

Signaltafeln sind Schluesselunterlagen von meist sehr begrenzter Grosse (durchschnittlich etwa 10 bis 50 Positionen) mit willkuerlich gewaehlten Schluesselzahlen fuer bestimmte haeufig gebrauchte Woerter, Befehle und Meldungen stereotyper Art. Zumeist handelt es sich um Schluesselmitel der fliegenden Verbaende fuer den Boden-Bord-Verkehr. Sie werden von den Verbaenden oft nur handschriftlich erstellt und nicht um ueblichen Sinne ueberschluesst, sondern immer neu konstruiert. Infolge der kurzen Laufzeit dieser Tafeln (bei Boden-Bord meist nur ein Feindflug) ist eine Rekonstruktion nur selten moeglich. In guenstig gelagerten Faellen aber auch nur bei enger Zusammenarbeit mit Funkern und Betriebsauswertern und unter Heranziehung der Tagesmeldungen. Wegen der erwachten kurzen Laufzeit sind auch Beute-Tafeln aus abgeschossenen Feindmaschinen unbrauchbar.

f) Das Satzbuch ("kod").

Das Satzbuch ist die Schluesselunterlage der Sowjets. Es ist zu erwachen, dass eine klare Grenze zwischen "Tafel" und "Satzbuch" nicht besteht. So bezeichnen z.B. selbst die Sowjets einige ihrer mehrseitigen Schluesselunterlagen (also Satzbuecher) oft noch als "Tafel".

Das Satzbuch erscheint bei den Sowjets in einer erstaunlichen Variationsfuelle in Bezug auf Wortschatz, Aufbau und Ueberschlueselungsmoeglichkeit. Neben Satzbuechern mit wenigen hundert Positionen sind Codes bis zu 30 000 Elementen im Gebrauch, neben lexikografischen und systematischen Unterlagen stehen unsystematische

TOP SECRET

TOP SECRET

tische und unalfabetische.

Folgende Abarten des Satzbuches koennen unterschieden werden:

aa) Das lexikografische Satzbuch.

Alle Elemente des Satzbuches sind nach Anfangsbuchstaben und darueber hinaus auch nach den zweiten, dritten usw. Buchstaben streng alfabetisch geordnet (wie im Woerterbuch).

bb) Das bedingt alfabetische Satzbuch.

Entweder: Die Ordnung der Positionen nach den Anfangsbuchstaben ist zwar gegeben, doch sind alle Elemente mit gleichen Anfangsbuchstaben weiterhin nicht eingeordnet, z.B. bei kleineren Satzbuechern, wo man alle Elemente mit demselben Anfangsbuchstaben bequem ueberblicken kann.

Oder: Die alfabetische Reihenfolge der Anfangsbuchstaben ist mehr oder weniger gestoert, doch sind alle Elemente auf denselben Anfangsbuchstaben auch nach den naechsten geordnet.

cc) Das unalfabetische Satzbuch.

Bei dieser Form von Satzbuechern ist sowohl die Entcodung als auch die Auf- grundstellung sehr stark erschwert.

dd) Das Satzbuch ohne Zahlenpositionen.

Die Zahlen erscheinen im Schluesstext klar und koennen meist nur durch ihre von der Chi-Gruppe abweichende Stellenzahl als solche erkannt werden. Zu- weilen werden die Klarszahlen auch durch eine Umschaltgruppe des Satzbuches an- zeigt.

ee) Das Satzbuch mit systematisch angeordneten Zahlenpositionen.

Die Zahlengruppen im Satzbuch sind steigend (seltener auch fallend) ange- ordnet. Sie befinden sich entweder zusammenhaengend an einer Stelle im Satzbuch

TOP SECRET

TOP SECRET

oder aber sie sind nach einem festen System im Satzbuch verteilt.

Bei dieser Form wird die Zahlendeutung sehr erleichtert. Auch kann die Aufgründstellung der Unterlage sehr erheblich beschleunigt werden.

ff) Das Satzbuch mit willkuerlich eingestreuten Zahlenpositionen.

Entweder: sind die Zahlen zwar steigend bzw. fallend aber mit ganz willkuerlichen Abstaenden voneinander ins Satzbuch eingestreut,

Oder: die Zahlen sind im Satzbuch vollkommen willkuerlich verteilt.

In diesem Fall ist die Deutung der Zahlenpositionen sehr schwer, eine Aufgründstellung mit ihrer Hilfe unmoeglich.

gg) Das Satzbuch mit eindeutigen Positionen.

In diesen Satzbuechern ist jede Position eindeutig, d.h. jede Position bedeutet in allen Faellen immer dasselbe. Die Existenz von Umschaltgruppen ist unnoetig.

hh) Das Satzbuch mit mehrdeutigen Positionen.

Alle oder auch nur ein Teil der Positionen sind mehrdeutig. Z.B. ist man in der Lage, von einer Position nur den Anfangsbuchstaben zu gebrauchen ^{x)} oder aber die Zeilen sind in eine linke und rechte Haelfte mit mehr oder weniger verschiedenen Bedeutungen geteilt. Zur genauen Festlegung der gewuenschten Moeglichkeit sind mindestens zwei Umschaltgruppen vorhanden, die die Eindeutigkeit der Chi-Gruppen im Spruch zu garantieren haben.

x) = sogenannter "Wortcode".

i) Das Satzbuch mit einfacher Positionsbelegung.

Jedes Element im Satzbuch ist nur einmal vorhanden; hat das Satzbuch also 500 Zeilen z.B., so sind in ihm tatsaechlich 500 verschiedene Sprachelemente enthalten.

TOP SECRET

TOP SECRET

kk) Das Satzbuch mit mehrfacher Positionsbelegung.

In diesem Falle sind einzelne Positionen (z.B. Buchstaben und haeufig gebrauchte Woerter) mehrfach vorhanden und koennen zur Vermeidung von statistischen Haeufungen immer abwechselnd gewaehlt werden.

Die vorstehend einzeln aufgefuehrten Merkmale tauchen natuerlich nicht in der angefuehrten reinen Form auf, sondern werden in der Regel miteinander gekoppelt und ergeben somit die verschiedensten Zusammenstellungen und Variationsmoeglichkeiten.

g) Das Formblatt. ("forma nr. ...")

Formblaettersprueche enthalten Meldungen verschiedenster Art (z.B. Treibstoffbestand und -Bewegung, Personal- und Geraetemeldungen, Meldungen ueber Flugplatzbeschaffenheit und -belegung) nach einem vorliegenden festen Schema. In der Regel werden Klarzahlen gebraucht.

In erster Linie interessieren die Formmeldungen durch das Auftauchen von klaren Einheitsnummern und Staerkezahlen, doch kann auch die laufende Verfolgung etwa von Treibstoffmeldungen wichtige Aufschluesse geben. Die restlose Deutung der Formblaetter stoesst auf grosse Schwierigkeiten, meist muss man sich mit Deutungen in ganz grossen Umrissen zufrieden geben, die auswertemaessig auch meist ausreichen.

Die Formblatt-Entzifferung und -Bearbeitung ist aus Gruenden der Zweckmaessigkeit der Auswertung direkt unterstellt gewesen.

h) Der Kartenschluessel

Die verschiedenen regionalen und generellen Kartenschluessel (Planquadrate) wurden ebenfalls im Rahmen der Auswertung bearbeitet. Bei dieser Bearbeitung sind keine wesentlichen Schwierigkeiten aufgetaucht.

TOP SECRET

TOP SECRET

1) Der Wetterschlüssel (meteo. "ans")

Den sowjetischen Wetterspruechen ist der internationale Kopenhagener Wetterschlüssel unterlegt, der durch all 6 Stunden wechselnde Wuermer (Verwuerfelung von Wurmtafeln und freie Wahl der Einsatzpunkte) ueberschlüsselt wird.

Die Bearbeitung des generellen Wetterschlüssels lag in den Haenden von OKL Chef Wetterdienst, die Abteilungen des H-Regiments hatten lediglich 1 bis 2 sukzessive Wetterschlüssler von Chef Wetterdienst, die das laufende Material auf Grund der taeglichen Ausstrahlungen von Chef Wetterdienst bearbeitet haben.

k) Die Uebungstafel.

Uebungstafeln sind Tafeln mit willkuerlichen Zahlen oder gemischten Gruppen, die zur Konstruktion von Uebungsspruechen benutzt werden. Die Gegenstelle kann auf Grund einer Kenngruppe im Spruchtext den Uebungstext rekonstruieren und somit die Aufnahmequete des Uebungsspruches kontrollieren.

Uebungssprueche sind zuweilen auch von eingesetzten Verbaenden der Fliegertruppe abgesetzt worden, offensichtlich nicht nur aus Uebungs- sondern auch als Verschleierungsgruenden.

3. Die Ueberschlüssellung.

a) Allgemeines.

Durch die Ueberschlüssellung wird die wichtigste Taetigkeit des E-Kannes, das Ausziehen der Chi-Elemente und ihr Vergleich untereinander, gehemmt. Sie zwingt ihn zu zeitraubenden Identitaetsvergleichen und Reduktionsversuchen. Unter Umstaenden verwischt sie alle Gleichheiten und verhindert das Mitlesen ueberhaupt. (z.B. individuelle Wurmtueberschlüssellung).

Die Sowjets machen von der Ueberschlüssellung weitgehendsten Gebrauch und haben es auf diesem Gebiet besonders in den letzten Jahren zu einer

TOP SECRET

TOP SECRET

beachtlichen Geschicklichkeit gebracht.

In diesem Zusammenhang sei nur erwähnt, dass in der Regel die einzelnen Code-Gruppen durch mehrere Schlüsselreihen gleichzeitig bestimmt wird. Darüber hinaus wird zusätzlich durch die Erhöhung des Stellenwertes (z.B. Bereichsueberschlüsselung) das statistische Bild stark verwischt und aufgelöst.

b) Der Ueberschlüsselungswechsel.

Je häufiger der Ueberschlüsselungswechsel, desto grösser die Zersplitterung des Chi-Materials.

In der Regel werden die gebrauchten Ueberschlüsselungsreihen in besondere dafür vorgesehene freie Stellen und Felder der Schlüsselunterlage hineingeschrieben. Oder aber die Schlüsselreihen liegen gedruckt vor und können direkt an das Satzbuch oder die Tafel angelegt werden ("wkładyschi").

aa) Die langfristige Ueberschlüsselung.

Bei längerer Laufzeit einer Ueberschlüsselung (mehrtaetig oder taeglich) werden die Ueberschlüsselungsdaten durch die vorgesetzte Dienststelle meist befohlen. Die Bekanntgabe der Ueberschlüsselungsreihen im Befehl des zuständigen Nachrichtenfuehrers (etwa fuer einen Monat im voraus) und des jeweiligen Zeitpunktes fuer den Wechsel (meist 12 oder 24 Uhr - massgebend ist die taktische Uhrzeit des Spruches) gemengt vollauf, um den reibungslosen Ablauf der Schlüsselarbeit zu garantieren.

bb) Die kurzfristige Ueberschlüsselung.

Ist ein schnellerer Ueberschlüsselungswechsel vorgesehen, so wuerde die Festlegung der Ueberschlüsselungsdaten im voraus auf grosse organisator-

TOP SECRET

TOP SECRET

ische Schwierigkeiten stossen. Deshalb wird dem Verschluessler die Moeglichkeit gegeben, fuer jeden einzelnen Spruch eine ganz willkuerliche Ueberschluesselung - im Rahmen des gegebenen Systems natuerlich - selbst zu wahlen. Diese willkuerliche Wahl der Ueberschluesselung wird der Gegenstelle im Spruch durch die sogenannte Kenngruppe (Indikator) bekanntgegeben.

c) Die Kenngruppe (der Indikator).

Aus den zur Verfuegung stehenden Schluesselreihen, die zu Ueberschluesselungstafeln, Trammeln, usw. zusammengefasst sind, werden die gewaehlten Reihen, Trammeln, Bereichsueberschluesselungen usw. durch Kennzahlen eindeutig bestimmt. Die Zusammenfassung der notwendigen Kennzahlen erscheint dann an einer vorher festgelegten Stelle des Chi-Spruches als Kenngruppe, die in vielen Faellen durch Blender getarnt ist, um sich nicht von den anderen Chi-Gruppen des Spruches zu unterscheiden.

d) Das Ueberschluesselungssystem.

Die Zusammenfassung aller zur Ueberschluesselung notwendigen Zahlenreihen und Arbeitsanweisungen macht das Ueberschluesselungssystem aus.

In groesseren Zeitabtaenden - etwa monatlich - werden die Zahleninhalte der einzelnen Unterlagen geaendert. Zuweilen wird auch das ganze Ueberschluesselungssystem fuer eine Unterlage radikal veraendert, d.h. man veraendert nicht nur die Zahleninhalte der einzelnen Ueberschluesselungsbehele sondern fuehrt ganz neue Arbeitsgaenge ein. Der Wechsel eines Ueberschluesselungssystems bei gleicher Schluesselunterlage fuehrt erst durch einen nachtraeglichen Vergleich der bereits gut ausgearbeiteten Unterlage zur Identifizierung.

TOP SECRET

TOP SECRET

Einen Begriff von der Vielfalt der Ueberschluesselungssysteme geben die Beschreibungen der Verfahren in der Anlagen-Karte (Teil 2).

III. KURZE GESCHICHTLICHE ENTWICKLUNG DER SOWJETISCHEN FLIEGER-VERFAHREN UND DIE ERFOLGE DER DEUTSCHEN ENTZIFFERUNG.

A. Die Entwicklung bis zum Kriegsausbruch 1939.

Charakteristisch war der allgemein sehr geringe Spruchabsatz, der zum Teil auch noch als Uebungsverkehr identifiziert werden konnte. Die Uebungsprueche wurden aus Uebungstafeln herausgelesen; in einigen Faellen ist die Rekonstruktion dieser Uebungstafeln gelungen.

Trotzdem reichte aber das Material aus, um ein Feindbild - wenn auch in groben Umrissen - zu erstellen.

1. Die generelle 2-Z-Tafel.

Der Grossteil des Materials wurde nach einer 2-Z-Tafel verschluesselt, die in der Hauptsache ein systematisch aufgebautes Alphabet enthielt. Obwohl diese Tafel urspruenglich nur als Schluesselbehelf des Funkers and der Taste zur Abwicklung des Verstaendigungsverkehrs gedacht war, wurden auch die meisten anderen Sprueche nach diesen Tafeln verschluesselt. Dieses wurde vermutlich gemacht, um das 4-Z-Verfahren, den sogenannten "Kommandeur-Code", nicht vorzeitig zu verwenden und dadurch zu kompromittieren.

Die Ueberschluesselung der 2-Z-Tafel wurde mit Hilfe zweier Zahlenreihen ausgefuehrt. Diese Reihen wurden aus Systemtafeln herausgelesen, wobei jeder Militaerbezirk ueber eigene Tafeln verfuegte. Die 2-Z-Tafel war etwa 1 Jahr in Kraft, die Systemquadrate wurden monatlich gewechselt, die Ueberschluesselungen -

TOP SECRET

TOP SECRET

fuer jedes Funknetz gesondert - taeglich. Die Schluesselsicherheit war ausserst gering.

2. Der generelle 3-Z-Fliegerachluessel.

Das 3-Z-Verfahren fuer den ausschliesslichen Gebrauch innerhalb der Fliegertruppe und zwar insbesondere fuer den Boden-Bord-Verkehr und den Verstaendigungsverkehr der Bodenstellen wurde zwar sehr selten gebraucht, bereitete aber der Entzifferung keine wesentlichen Schwierigkeiten, da sowohl Satzbuch als auch Ueberschluesselung ziemlich primitiv gewesen sind. (Alphabetisches Satzbuch mit 1000 Positionen, taegliche Seitenueberschluesselung, einige Zeilen Ueberschluesselungsvarianten).

3. Das generelle 4-Z-Stabsverfahren.

Das 4-Z-Satzbuch war alphabetisch aufgebaut, hatte 50 bis 100 Seiten zu je 100 Zeilen und wurde nach Tauschtafeln ueberschluesselt. Hierbei handelt es sich um das generelle Verfahren zum Schluesseln taktischer Sprueche auch fuer die Staabe der Fliegertruppe. Dieses Verfahren wurde im Russischen als Kommandeur-Code bezeichnet.

Das Satzbuch wurde in der Regel zu den Fruehjahrsmanoevern gewechselt und nur waehrend dieses Manoevers selbst zu Uebungszwecken verwendet. Diese kurze Anwendungszeit genuegte aber um den Einbruch zu erzielen und die Sprueche mitzulesen - trotz meist sehr schlechter Empfangsverhaeltnisse. Interessanterweise waren die Spruchtexte oft sehr stereotyp gehalten; nachtraegliche Vergleiche haben ergeben, dass ein Teil dieser Texte aus einem Heft mit taktischen Uebungstexten gestaan haben muss.

TOP SECRET

TOP SECRET

4. Das generelle 5-Z-Wurverfahren.

Dieses Satzbuch mit etwa 30000 Positionen wurde mit einem Zahlensystem ueberschlüsselt. Es konnte infolge des sehr geringen Spruchanfalls weder in den Einzelheiten analysiert, geschweige denn mitgelesen werden. Dieses Verfahren wurde ebenfalls alljaehrlich gewechselt.

B. Die Besetzung Ostpolens im September 1939.

1. 2- und 3-Z-Schlüssel.

In der Wahl dieser Schlüsselmittel und ihrer Bearbeitung koennen keine neuen Gesichtspunkte aufgezeigt werden.

2. Das 4-Z-Stabsverfahren.

Waehrend des Eirmarsches der Roten Armee in Ostpolen schwoll das Material fuer den "okk 5" (lexikografisches Satzbuch mit 5000 Positionen und un-systematischer Tauschtafel-Ueberschlüssellung) derartig an, dass die regionalen Tauschtafeln ohne wesentliche Schwierigkeiten erstellt und die Masse des Spruchmaterials laufend mitgelesen werden konnte.

Die Frucht dieser Arbeit war ein umfangreiches und im Fuehrungsstab der Luftwaffe viel beachtetes Werk ueber die Besetzung Ostpolens mit wertvollen Erkenntnissen auch ueber die Fliegertruppe der Roten Armee.

3. Das 5-Z-Wurverfahren.

Auch in dieser Periode konnte das laufende 5-Z-Verfahren mangels Material zwar analysiert, aber nicht mitgelesen werden.

TOP SECRET

TOP SECRET

C. Der Finnische Winterkrieg 1939/40.

1. 2-, 3- und 4-Z-Verfahren.

wurde laufend mitgelesen, sonst keine besonderen Feststellungen.

2. Das 5-Z-Wortverfahren.

Das 5-Z-Verfahren konnte erstmalig, wenn auch mit Zeitverzögerungen, mitgelesen werden. Es handelte sich um ein 5-Z-Satzbuch mit etwa 25000 Elementen und charakteristischen Zeilenwerten. Die Ueberschlüsselung erfolgte anhand von Zahlentafeln, die mehrfach gebraucht wurden.

Dank der mitgelesenen Sprueche konnte ein ganz klares Feindbild gewonnen werden. So konnten auch die Erkenntnisse und Erfolge des sehr exakt arbeitenden finnischen H-Dienstes sehr oft in eine fuer die Rote Armee geradezu verheerende Waffenwirkung umgesetzt werden.

In einer nach dem Finnland-Feldzug herausgegebenen gedruckten Arbeitsanweisung fuer die Chiffrier-Offiziere der Roten Armee wurde ihre eigene Arbeit einer sehr scharfen Kritik unterzogen. Die Erfolge des finnischen H-Dienstes wurden aber fast ausschliesslich auf die eigene Sorglosigkeit zurueckgefuehrt, die Schlusssicherheit der Verfahren wurde nach wie vor erheblich ueberschaetzt.

D. Der Ostkrieg 1941/45.

1. Die Erfolge der deutschen Entzifferung.

Wahrend der sowjetischen Vorbereitungen zum Waffengang mit dem deutschen Reich wurde das sowjetische Chiffrierwesen auf Grund der boesen Erfahrungen des finnischen Winterkrieges in fieberhafter Eile reorganisiert. Diese Reorganisation hat sich bereits vor Beginn der Feindseligkeiten und dann im Verlaufe des Ostkrieges immer staerker ausgewirkt und der deutschen Entzifferung grosse Schwierigkeiten bereitet.

TOP SECRET

TOP SECRET

Trotz allem konnte der hoeheren Fuehrung vor Beginn des Ostfeldzuges ein detailliertes Feindbild ueber den Aufmarsch der sowjetischen Fliegertruppe unterbreitet werden. Die deutsche Entzifferung blieb auch weiterhin stets auf dem Laufenden und hat wesentliche Vorspruenge des sowjetischen Chiffrierdienstes immer wieder ohne grossere Zeitverluste aufzuholen vermocht. Die Erfolge waren offensichtlich. Seit Beginn des Ostfeldzuges sind ueber 900 grossere Verfahren der sowjetischen Fliegertruppe gelesen worden, die Anzahl der mitgelesenen Primitivschlüssel geht in die tausende.

Abgesehen vom 5-2-Material konnte die Masse der sowjetischen Fliegersprüche (75 bis 90%) laufend bzw. nach tragbaren Zeitverlusten mitgelesen werden. Insbesondere konnte das Spruchmaterial der Bodenorganisation fast restlos ausgewertet werden, die Schlüsselunterlagen waren in der Regel bis zu 90% gedeutet. Der Spruchanfall der fliegenden Verbände war wesentlich geringer, die Einbruchsmöglichkeiten unguenstiger und die Spruchinhalte allerdings auch unwesentlicher.

Das nicht mitzulesende Material bestand in der Hauptsache aus Einzelsprüchen nicht gedeuteter Netzsugehoerigkeit.

Zur Veranschaulichung der Arbeitserfolge der Entzifferung werden in der Anlage die Arbeitsergebnisse 1944/45 der III./Ln.Regiment 353 (Suedabschnitt der Ostfront) statistisch festgehalten. Im Mittelabschnitt war der absolute Spruchanfall teilweise geringer, die Entzifferungsergebnisse prozentuell gleich gut; im Nordabschnitt waren auf Grund der regionalen Bedingungen sowohl Spruchanfall als auch der Prozentsatz der entzifferten Sprueche geringer.

Seit 1941 musste die deutsche Luftwaffenentzifferung an der Ostfront stets durchschnittlich etwa 100 grossere Schlüsselvefahren gleichzeitig bearbeiten.

TOP SECRET

TOP SECRET

2. Die charakteristischen Veraenderungen der sowjetischen Chiffriermethod

a) Abschaffung der generellen Schluesselverfahren - Einfuehrung von Regionalverfahren

Bis auf das 5-2-Wurverfahren wurden alle anderen generellen Schluesselmittel aus dem Verkehr gezogen. Jedes Netz erhielt seine eigenen Schluesselunterlagen, die durch den Chiffrieroffizier der Hauptfunkstelle nach allgemeinen Direktiven und Anregungen der Chiffrierstelle der Roten Armee und der sonstigen vorgesetzten Fachinstanzen erstellt werden. Vielfach sind innerhalb eines Netzes sogar mehrere Spezialverfahren gleichzeitig im Gebrauch (Sonderschluessel fuer den Nachschub, regionale Wetterschluessel, Formblaetter fuer Meldungen der verschiedensten Art usw.). Auch nach einem Unterstellungswechsel behielten die Verbaende in der Regel ihr altes Schluesselverfahren bei.

Durch diese Massnahme erhielt die Fliegertruppe erstmalig und ganz allgemein die Moeglichkeit zum Gebrauch eigener Verfahren, die fuer die Fliegertruppe besonders zugeschnitten werden koennten (Differenzierung des Wortschatzes, Beruecksichtigung der besonderen Verhaeltnisse beim Boden-Bord-Verkehr usw.).

Durch die Dezentralisation der Schluesselerstellung wurde das fuer die Sowjet-Union hoechst schwierige Problem des Schluesselnachschubes gut geloest.

Die Vielfalt der Schluesselmittel wirkt auf den Entzifferer hoechst verwirrend und macht die Organisation eines besonderen Schluesselerkennungsdienstes notwendig, der insbesondere dann sehr wichtig ist, wenn die Auswertung es nicht vermag, laufend gute und einwandfreie Netzdeutungen zu geben. Die Steigerung der Neubearbeitungen verlangt eine starke Erhoehung des ausgebildeten E-Personals und veraendert das Verhaeltnis zwischen Fachpersonal mit guten Sprachkenntnissen und Hilfspersonal ohne Sprachkenntnisse zu Ungunsten des Letzteren.

TOP SECRET

TOP SECRET

b) Verkuerzung der Laufzeit der Verfahren

Die Laufzeit der einzelnen Verfahren wurde stark herabgesetzt. Anfang 1945 konnte man mit einer durchschnittlichen Laufzeit von etwa 4 Monaten rechnen. Die Schwankungen sind allerdings bis zum Schluss sehr stark geblieben; es hat Luftarmeen gegeben, die ihre Verfahren wesentlich laenger laufen liessen (9 bis 12 Monate). andererseits sind auch viele Schluesselunterlagen nur wenige Wochen gebraucht worden.

c) Komplizierung der Schluesselunterlagen

Die Schluesselunterlagen der Regionalverfahren behielten eine verhaeltnissaessig geringe Positionszahl (durchschnittlich 1000). Doch wurden alphabetische und systematische Unterlagen in der Regel durch unalphabetische und unsystematische ersetzt. Unterlagen auf der Grundlage von Buchstaben oder Silbentypen nahmen ab, Wortcodes nahmen zu. Durch diese Entwicklung werden Entcodungsarbeiten und Aufgrundstellungen wesentlich erschwert.

Auf Grund der starken Differenzierung der einzelnen Verfahren wird der Wortschatz ebenfalls immer spezieller. So sieht z.B. das Satzbuch einer Aufklaerereinheit anders aus als das eines Flieger-Boden-Bezirks.

d) Komplizierung der Ueberschluesselungssysteme

Der Differenzierung der Ueberschluesselungsmethoden wurde allgemein eine sehr grosse Bedeutung beigegeben. Die Ueberschluesselungssysteme sind immer unsystematischer und komplizierter geworden.

Das Erkennen des Ueberschluesselungssystems wird deshalb sehr erschwert, so gelingen Reduktionen viel spaeter, u.U. sogar garnicht, wenn auch das entsprechende Chi-Material mitgelesen werden kann.

TOP SECRET

TOP SECRET

Zuweilen werden bei der Verwendung einer Schluesselunterlage nach gewissen Zeitabstaenden die Ueberschluesselungssysteme so veraendert, dass die Identitaet des Satzbuches lange Zeit unerkannt bleibt.

e) Die Aehnlichkeit der Schluesselsysteme.

Gerade nach der Einfuehrung der Regionalverfahren konnte immer wieder das Auftauchen und die anschliessende Ausbreitung gewisser neuer Schluesselprinzipien ueber die ganze Front beobachtet werden. Dabei hat sich gezeigt, dass die Schluesselverfahren eines Grossraumes, die Verfahren einer Luftarmee etwa, ganz spezifisch typische Merkmale aufweisen im Bezug auf den Aufbau der Satzbuecher, die Ueberschluesselungssysteme, die Lesarten, die Laufzeiten der Unterlagen und Ueberschluesselungstafeln, der Kenngruppen- und Signalgruppenanwendung.

Vielfach hat diese Beobachtung die analytisch konstruktive Arbeit der Entzifferung wesentlich erleichtert: Das erstmalige Auftauchen eines neuen Schluesselprinzips fuehrte stets zur berechtigten Annahme, dass sich dieses Prinzip in der allernaechsten Zeit auch auf die Schluesselgestaltung des ganzen Raumes auswirken wuerde.

f) Abschaffung der generellen 2-Z-Tafeln und Umschulung auf Q-Gruppen

Der Aufbau der generell gebrauchten 2-Z-Tafeln fuer den Verstaendigungsverkehr wurde immer schwieriger und unsystematischer; trotzdem konnte das Material stets mitgelesen werden. Schliesslich wurde die Verwendung dieser Tafeln ganz eingestellt und die Funker auf die Benutzung der unwesentlich variiert internationalen Q-Gruppen umgeschult. Seitdem tauchen 2-Z-Schluessel nur sehr selten als regionale Primitivschluessel auf.

TOP SECRET

TOP SECRET

g) Individuelle Spruchueberschlüsselung.

Der selten, meist taegliche Ueberschlüsselungswechsel wurde durch eine individuelle Ueberschlüsselung des einzelnen Spruches abgelöst, die im Einzelspruch durch Schlüsselgruppen angezeigt wird. Diese Massnahme hat eine weitgehende Zersplitterung des Chi-Materials bewirkt.

h) Verwendung von Blendern und Kontrollzahlen.

Durch Blender bzw. Kontrollzahlen wird die Form der Schlüsselunterlage unter Umstaenden sehr stark verdeckt.

i) Variierung der Lesart.

Während vorher die Chi-Gruppe bzw. Position ganz allgemein ABCDE gelesen wurde, kann nunmehr bei vielen Verfahren eine immer wilder um sich greifende Unregelmässigkeit der Lesarten festgestellt werden.

Diese Tatsache kann schon bei der Analyse des Systems grosse Schwierigkeiten bereiten.

k) Unterdrueckung der Systematik.

Die zweifellos vorliegende Neigung des Russen zur systematischen Konstruktion seiner Schlüsselunterlagen, die vielfach nicht nur unnoetig sondern geradezu schaedlich ist, wird in der letzten Zeit anscheinend bewusst unterdrueckt bzw. zurueckgedaemt.

1) Das 5-Z-Wurverfahren.

Als einziges allgemeines Verfahren fuer Heer und Fliegertruppe wird bei den hoeheren Staeben ein unalfabetisches 5-Z-Satzbuch mit etwa 25000 Elementen beibehalten und im langsam steigenden Masse angewandt. Die Satzbuoecher werden

TOP SECRET

TOP SECRET

nach etwa 3 bis 4 Monaten ausgewechselt. Ende 1941 wurden fast gleichzeitig 2 oder 3 verschiedene Satzbu~~cher~~ erbeutet, die noch nicht in Gebrauch gewesen waren.

Die Anwendung von sogenannten "allgemeinen Wurmtafeln", d.h. mehrfach gebrauchten Tafeln, wenn auch mit verschiedenen Einsatzpunkten, wurde durch die ausschliessliche Verwendung von sogenannten "individuellen" Wurmtafeln abge-
loest. D.h., jede Wurmtafel wird tatsaechlich nur einmal gebraucht und nach dem Gebrauch sofort vernichtet. In diesem Fall ist die Schluesselsicherheit absolut. Ein Einbruch in den einzelnen Spruch ist auch bei Vorlage eines Beute-Satzbuches nur dann moeglich, wenn in der Belieferung der einzelnen Funkstellen mit individuellen Wurmtafeln eine Stockung eintritt und der Verschluessler deshalb genoetigt ist, eine Tafel doch mehrfach zu benutzen. Die umfangreiche Nachschuborganisation der Sowjets kann aber als mastergueltig bezeichnet werden, Doppelueberschluesslungen kamen so gut wie garnicht vor.

Bei dieser Sachlage haben in den letzten Kriegsjahren die zusammengefaassten Bemuehungen sowohl der Heeres- als auch der Luftwaffen-Entzifferung zu keinem lohnenden Ergebnis gefuehrt, weil ja nur die sehr seltenen unvorschriftsmaessig verschluesselten Sprueche mitgelesen werden konnten. Schliesslich wurde die Bearbeitung dieses Verfahrens eingestellt. Trotz der Aussichtslosigkeit, 5-Z-Sprueche mitlesen zu koennen, ist ihr Empfang aber nicht unterbrochen worden, weil die Kenngruppen dieser Sprueche ("Bloknot") fuer die Betriebsauswertung wertvolle Unterlagen zur Netzdeutung darstellen.

Zum Glueck zeigte das laufende Mitlesen der 5-Z-Sprueche in den ersten Jahren des Ostkrieges, dass der Spruchinhalt - auswertemaessig gesehen - nicht sehr wertvoll gewesen ist. Insbesondere sind taktische Plaene oder Einsatzbefehle nach diesem Verfahren ebenfalls kaum verschluesselt worden. In der Regel

TOP SECRET

TOP SECRET

handelte es sich um Lage- und Nachschubmeldungen und den Nachrichtenaustausch der politischen Truppenfuehrung. Die wichtigsten all dieser Nachrichten tauchten dann meist auch nach anderen Verfahren verschluesselt auf.

m) Das Auftauchen von Versatzzschluesseln.

In den ersten Monaten 1945 haeuften sich beim Heer die Anzeichen fuer eine generelle Einfuehrung primitiver Versatzzschluessel (Schablonen), offensichtlich als Ersatz fuer die bisher ueblichen 2-Z-Ersatzzschluessel. Im Falle der Richtigkeit dieser Annahme kann erfahrungsgemaess auch bei der Fliegertruppe mit dem Auftreten derartiger Schluessel gerechnet werden.

n) Die Anwendung von Maschinenschluesseln.

Die Verwendung von Maschinenschluesseln ist bis jetzt ganz gering und nicht ins Gewicht fallend. Waehrend der Belagerung Odessas wurde ein 5-B-Verfahren beobachtet; bei dem sehr geringen Materialanfall ergab die Analyse die Anwendung eines Maschinenschluessels. Ein weiteres 5-B-Verfahren des Oberkommandos der Fernkampfflieger (ADD) duerfte wohl auch Maschine sein, konnte aber ebenfalls nicht bearbeitet werden, weil das Material auch zu den notwendigen analytischen Untersuchungen nicht ausgereicht hat.

IV. ORGANISATION UND ARBEITSWEISE DER DEUTSCHEN ENTZIFFERUNG

A. Kurzer geschichtlicher Rueckblick auf die organisatorische Entwicklung der deutschen Luftwaffen-Entzifferung Ost

Waehrend der Vorbereitungszeit zur Aufstellung des H-Apparates der Luftwaffe im Jahre 1936 wurden die allerersten fuer eine Entzifferungsarbeit vorgesehenen Reichsangestellten (bis zum Kriegsausbruch ausschliesslich Zivilisten) zum Zwecke einer grundlegenden Ausbildung zu den festen H-Stellen des Heeres im Osten kommandiert. Das Ergebnis dieser Ausbildung war duerftig, weil das Heer

TOP SECRET

TOP SECRET

in der Weitergabe auch der primitivsten Erkenntnisse sehr zurückhaltend gewesen ist und andererseits auch die kommandierten Kräfte in den meisten Fällen wesentliche Voraussetzungen für ihre Arbeit nicht besaßen, da die Personalbearbeiter bei der Einstellung neuen Personals sehr unsachgemäß vorgegangen sind und zahlreiche Leute eingestellt hatten, die für den Beruf eines Entzifferers sich als denkbar ungeeignet erwiesen. Die Aufstellung einer arbeitsfähigen und erfolgreichen Entzifferung wurde erst im Laufe der nächsten Jahre mühevoller Arbeit, ohne fremde Hilfe und von innen heraus, unter Abstossung zahlreicher unbrauchbarer Elemente, erreicht.

Mitte 1937 arbeiteten in der Chi-Stelle Ob.d.L. 4 Entzifferer gegen die Sowjet-Union. Die anderen Oststaaten wurden entweder sehr oberflächlich, zum Teil nebensächlich von den Sowjet-Bearbeitern, oder aber überhaupt nicht bearbeitet. Die E-Gruppen der Aussenstellen des Luftwaffen-H-Dienstes (Tarnname "Wetterfunkempfangsstelle") bestanden ebenfalls aus wenigen schlecht ausgebildeten und oft minderwertigen Kräften. Eine ernsatznehmende Neuentzifferung bildete sich anfangs nur bei der Chi-Stelle. Die Aussenstellen waren kaum imstande, das Chi-Material nach vorliegenden Schlüsselunterlagen zu bearbeiten.

Bei Kriegsausbruch 1939 waren die E-Gruppen sowohl bei der Chi-Stelle als auch bei den Aussenstellen auf je etwa 10 Mann angewachsen, sie wurden in die neu aufgestellten Horchkompanien eingebaut. Der Ausbildungsstand der einzelnen Entzifferer wurde durch Arbeitsbesprechungen, kurzfristige Lehrgänge und durch Austauschkommandierungen der Spitzenkräfte zu Einweisungszwecken laufend verbessert.

Während der Besetzung Ostpolens im Herbst 1939 und während des finnischen Winterkrieges 1939/40 wurden die besten Kräfte der Aussenstellen bei der Chi-Stelle

TOP SECRET

TOP SECRET

Zusammgezogen, weil die E-Gruppen der Aussenstellen sich nicht in der Lage zeigten, das laufende, fuer die geringe Mitarbeiterszahl gewaltige Material schnell und praezise genug zu bearbeiten. Ausserdem wurde bei der Chi-Stelle zur Bearbeitung des 5-Z-Verfahrens waehrend des finnischen Winterkrieges eine Rechnergruppe von etwa 20 Mann (ohne Sprachkenntnisse) eingesetzt, die auch in der Folge den Stamm fuer die Wurnbearbeitungen bildete.

Zu Beginn des Ostfeldzuges wurde das Referat E 1 der Chi-Stelle (spaeater E-Abteilung des Regiments 353) auf etwa 40 Mann und im Laufe des Krieges auf etwa 90 vergruessert, worunter sich allerdings auch weibliche Arbeitskraefte befunden haben. Die Belegschaften der Aussenstellen (spaeater E-Abteilungen der Auswertekompanien) stiegen auf etwa 40 bis 60 Mann, eine Durchsetzung mit Frauen erfolgte allerdings - bis auf einige seltene Ausnahmen - nicht.

Auch die H-Kompanien bei den einzelnen Flieger-Korps, kurz Korps-Kompanien genannt, hatten kleine E-Gruppen, die allerdings leider mit sehr schlecht ausgebildetem Personal besetzt werden mussten und auf Grund des kleinen Arbeitshorizontes ihr niedriges Fachniveau behielten, wenngleich ihre Arbeitserfolge durchaus nicht zu unterschaezen waren.

In den letzten Kriegsmonaten ist ein Teil des wenig qualifizierten E-Personals an die kampfende Truppe abgegeben worden.

Waehrend zu Beginn des Krieges das Schwergewicht der Arbeit zweifellos bei der Chi-Stelle gelegen hatte und immer wieder das damals nicht von der Hand zu weisende Projekt einer Zusammenfassung aller E-Kraefte bei einer Zentralentzifferungsstelle auftauchte, entwickelten sich im Verlauf des Krieges die

TOP SECRET

TOP SECRET

E-Abteilungen bei den Luftflotten immer mehr und wurden auf Grund des Regionalschlus-
selsystems der Sowjets in die Lage versetzt, das vor ihrer Front anfallende Chi-
Material vollkommen selbstaendig zu bearbeiten.

Das Referat E 1 dagegen verlor immer mehr seine Bedeutung und sank zu
einem Archiv und organisatorischen Relais herab, obwohl es zum Teil ueber ein ganz
vorzuegliches E-Personal verfuegte. Als einzige Spezialaufgabe verblieb ihm die
Bearbeitung des 5-Z-Verfahrens, weil dieses Material eine regionale Bearbeitung
nicht vertrug. Doch schliesslich - nachdem die zusammengefasste Bearbeitung dieses
Materials zeitweise bei der Luftwaffe bzw. beim Heer vor sich gegangen war, wurde
die zwecklos gewordene Bearbeitung aufgegeben, womit das Referat seine letzte eigene
Aufgabe verlor.

B. Gedanken zur organisatorischen Idealform.

Die Stellungnahme zum Problem "Zentralisation oder Dezentralisation der
Entsifferung?" wird durch die augenblickliche Eigenart des sowjetischen Chi-Mater-
ials (starke Differenzierung und regionale Aufsplitterung der Schluesselmittel) be-
stimmt.

Bei einer Zentralisation waere wohl jegliche sonst unvermeidbare Doppel-
arbeit vermieden, auch koennte der Personaleinsatz rationeller gestaltet werden.
Doch waeren die Nachteile viel groesser, so lange es unmoeglich erscheint, den
Funkempfang wegen der Frontlaenge im Osten von einer Stelle aus zu betreiben.
Denn: Bei dem verspaeeteten Einlaufen des Spruchmaterials in der Zentrale, das
durch das nicht ausreichende und vielfach gestoerte Nachrichtennetz verursacht
wird, verliert das Material an Aktualitaet. Ausserdem entstehen bei jeder Spruch-
uebermittlung auf dem Fernschreibwege zusaetzliche Fehlerquellen, die erfahrungs-
gemess sehr hinderlich sein koennen und den Wert des Chi-Materials stark druecken.

TOP SECRET

TOP SECRET

Darueber hinaus wuerde der unbedingt notwendige Kontakt zwischen H-Funker und Entzifferer vollstaendig unterbrochen werden.

Aus diesem Grunde kann die regionale Zusammenballung der Entzifferungskraefte bei den Luftflotten zur selbstaendigen Bearbeitung ihres Frontabschnittes tatsaechlich als die gluecklichste Loesung betrachtet werden. Aus der umfangreichen E-Abteilung des Regiments hatte aber ein kleiner Arbeitstab ausschliesslich fuer Organisations- und Ausbildungsfragen gebildet werden muessen; alle uebrigen E-Maenner haetten bei den Luftflotten wesentlich wertvollere Arbeit leisten koennen.

Eine weitere Zersplitterung der E-Kraefte ist aber nicht ratsam und zu vermeiden, soweit nicht abgesetzte Kompanien mit eigenem Aufgabengebiet (z.B. Fernkampfflieger oder Luftverteidigung) bestehen.

C. Organisation und Arbeitsweise einer E-Abteilung.

1. Die E-Abteilung einer Auswerte-Kompanie

In diesem Kapitel wird die Organisation und Arbeitsweise der E-Abteilung der Auswertekompanie einer Horch-Abteilung (Bataillon) skizziert.

Alles hier Gesagte gilt im Wesentlichen ebenso fuer die E-Abteilung des H-Regiments (frueher Referat E 1 der Chi-Stelle Ob.d.L.) als auch fuer die kleinen E-Gruppen der abgesetzten Kompanien mit besonderem Aufgabengebiet.

Die E-Abteilung bildet einen Zug der Auswerte-Komp. Leiter der Abteilung ist nach Moeglichkeit einer ihrer Wachoffiziere. Voraussetzung ist aber, dass der Leiter ein ueberragender Fachmann ist, der Dienstgrad spielt in diesem Falle nur eine untergeordnete Rolle.

TOP SECRET

TOP SECRET

2. Der Leiter der E-Abteilung (Chefentsifferer)

Er ist die Seele der ganzen Abteilung. Von ihm haengen Ausbildungsstand, Arbeitsfreudigkeit und Erfolg ab. Ist er nicht in der Lage, seine ueberragenden Fachkenntnisse staendig unter Beweis zu stellen, verliert er sehr bald die Achtung und das Vertrauen seiner Maenner. Die Erfahrungen mit Offizieren, die ohne oder mit nicht ausreichenden Fachkenntnissen die organisatorische Leitung einer E-Abteilung uebernehmen mussten, waren stets niederschmetternd. Denn: Eine organisatorische Taetigkeit (Personaleinsatz, Arbeitszeit, usw.) ohne tatsaechliche Fachkenntnisse fuehrt zu dauernden Fehlentscheidungen und wirkt sich im hoechsten Masse schaedlich aus.

Alle E-Arbeit ist Vertrauenssache, man kann weder einen Menschen zum Entziffern zwingen, noch den tatsaechlichen Arbeitsaufwand exakt messen, denn Arbeitsaufwand und Erfolg stehen bei der Entzifferung leider Gottes nicht immer im direkten Verhaeltnissen. Schon aus diesen Gruenden heraus muss der Chef alle seine Mitarbeiter nicht nur fachlich sondern auch charakterlich beurteilen koennen.

Durch taegliche, wenn auch kurze Ruecksprachen muss der Chef in der Lage sein, die Arbeit eines jeden einzelnen Mannes dauernd verfolgen zu koennen, um bei unvermeidlichen Stockungen mit Rat und Tat zur Verfuegung zu stehen. Bei diesen Ruecksprachen werden auch laufend organisatorische Missstaende und notwendig werdende personelle Umstellungen offenbar.

Besonders schwierige Probleme bearbeitet der Chefentsifferer persoenlich unter der Assistenz besonders guter z.b.V.-Leute. Er ist der Mann, der immer dabei ist, "wenn die Karre im Dreck steckt". "Laeuft der Wagen wieder", dann kann er sich getrost neuen Schwierigkeiten zuwenden und die Weiterbearbeitung des alten Verfahrens seinen Mitarbeitern allein ueberlassen.

TOP SECRET

TOP SECRET

Auf Grund der Geheimhaltung muss die Arbeit des Entzifferers nach aussen hin immer unscheinbar bleiben. Umso mehr ist es die Aufgabe des Chefentzifferers, durch gerechtes Lob auf seine Mitarbeiter erfrischend zu wirken und darueber hinaus dafuer zu sorgen, dass die Leistungen seiner Maenner auch "von oben" (etwa bei Besichtigungen) entsprechend gewuerdigt werden.

3. Der Schichtdienst

Waehrend des Krieges haben die Maenner der E-Abteilung ihren Dienst in zwei (Frueh- und Spaetschicht) oder in drei Schichten (durchgehender Dienst) versehen. Die genaue zeitliche Einteilung des Dienstes ist abhaengig vom Arbeitsanfall und von der Grosse der zur Verfuegung stehenden Raume und muss verhaeltismaessig haeufig den jeweiligen Erfordernissen neu angepasst werden.

Die Personalbesetzung der Schichten bedarf einer besonderen Sorgfalt, weil die Faehigkeiten der Mitglieder der Schicht sorgsam aufeinander abgestimmt werden muessen.

4. Der Schichtfuehrer

Die E-Schichten bewaeltigen die laufenden Entschluesselungs- und die leichteren Entzifferungsarbeiten. Der organisatorische Leiter der Schicht ist ein erfahrener und zuverlaessiger E-Mann, der als solcher fuer den gesamten Arbeitsprozess innerhalb der Schicht verantwortlich ist. Er verteilt die anfallende Arbeit nach den Weisungen des Chefentzifferers. Er muss die Schwierigkeit der Arbeitsvorgaenge beurteilen koennen, um Leerlauf oder Ueberlastung des einzelnen Mitarbeiters zu erkennen und zu regulieren. Da die Fuelle von organisatorischen Arbeiten den Schichtfuehrer fuer eine regulaere Entzifferungstaetigkeit wenig Zeit laesst und ein laengerer Einsatz als Schichtfuehrer seine Buerokratisierung bewirken wurde, ist von Zeit zu Zeit eine "Wachabloesung" angebracht. Aufgabe

TOP SECRET

TOP SECRET

des Chefentsifferers ist es nun, seine Maenner so zu erziehen, dass sie in der Betrauung mit dem Schichtfuhrerposten keinen "sozialen Aufstieg" sehen, sondern nur eine zeitlich begrenzte wenn auch ehrenvolle Berufung. Die Abloesung des Schichtfuhrers ist weder ein Misstrauensvotum noch eine Strafe und bezweckt lediglich die Erhaltung der Arbeitskraft des Einzelnen.

5. Der Entzifferer z.b.V.

Fuer zeitlich begrenzte und besonders schwierige Aufgaben werden vom Chefentsifferer aus den Schichtbesatzungen besonders erfahrene zuverlaessige und befahigte E-Maenner herausgezogen. Im Allgemeinen arbeiten sie im Tagesdienst und stehen dauernd in engster Verbindung mit dem Chefentsifferer. Diesen z.b.V.-Maennern wird in Bezug auf Arbeitszeit und Dauer mehr oder weniger freie Hand gelassen - soweit natuerlich nicht unvermeidliche militaerische Belange dagegen sprechen.

Die staendige Variierung der Zusammensetzung der z.b.V.-Belegchaft gibt die Moeglichkeit,

erstens: besonders befahigte Spezialisten auf ihren Sondergebieten einzusetzen und

zweitens: durch eine zweckentsprechende Arbeitsverteilung den Ausbildungsstand des Einzelnen zu erhoehen.

Eine Spezialisierung des Einzelnen ist nicht zu vermeiden. Sie ist an sich auch wuensenswert. Doch muss dafuer Sorge getragen werden, dass diese Spezialisierung nicht zur Einseitigkeit wird und die Mitarbeiter den notwendigen Gesamtueberblick verlieren.

TOP SECRET

TOP SECRET

6. Die Registratur

Bei der Ueberfuelle an Papier und der daraus entspringenden Gefahr einer Redaktionsstubenordnung ist die unermuedliche Arbeit einer straff aufgezogenen Registratur unerlaesslich. Sie besteht aus 1 bis 2 Mitarbeitern, die nach Moeglichkeit minimale Sprach- und Fachkenntnisse besitzen muessen, um nicht durch eine 100%ige Unkenntnis der Materie mehr Unheil anrichten als Ordnung zu stiften. Die Aufgaben der Registratur bestehen im folgenden:

Vorsortierung des anfallenden Spruchmaterials,

Zusammenlegung des Materials nach Netzen auf Grund der Spruchauszeichnung (Netznummer, Rufzeichendeutung) der Betriebsauswertung,

Zusammenlegung nach Verfahren auf Grund bekannter Signalgruppen und sonstiger Kennzeichen (Erkennungsbuecher der E-Abteilung),

Aussiebung des nicht interessierenden Spruchmaterials fremder Fronten und anderer Wehrmachtteile und ihre Weiterleitung an die zustaendigen Stellen bzw. ihre Vernichtung,

Sammlung nicht mitgelesenen Materials bis zur Inangriffnahme der Bearbeitung bzw. bis zur Loesung,

Weiterleitung des entzifferten Materials an die Auswertung,

Aufbewahrung der mitgelesenen Sprueche nach beendiger Auswertung (Sprucharchiv),

Geheimregistratur der Schriftstuecke, Fernschreiben und sonstigen Unterlagen.

Neben dieser Taetigkeit koennen die Registratoren im Bedarfsfall auch zu statistischen Hilfsarbeiten herangezogen werden.

7. Der "Bastler"

Es erscheint ratsam, bei jeder E-Abteilung einen Mitarbeiter zu haben, der die vielfaeltigen Ueberschliessungsbehelfe in Form von Schiebetafeln, Trammelalysystemen, Schluesselunterlagen usw. in einer zweckmaessigen und sauberen Form basteln kann und seinen Kameraden staendig zur Verfuegung steht. Durch diese

TOP SECRET

TOP SECRET

b) Die Erstellung des Ueberschluesselungssystems.

Auch die vorliegenden Ueberschluesselungsreihen muessen miteinander verglichen und zu einem zusammenfassenden System vereinigt werden.

6. Die Ausarbeitung

Durch Ueberarbeiten des nach erfolgter Auswertung in die E-Abteilung zurueckfliessenden Materials werden die Unterlagen durch weitere Positionsdeutungen vervollstaendigt.

Waehrend noch in den ersten Kriegsjahren der Einbruch als die wesentlichste entzifferungstechnische Arbeit angesehen werden konnte, hat sich nunmehr der Schwerpunkt der Arbeit immer mehr auf Systembearbeitung und Unterlagenerstellung verlagert.

E. Einige allgemeine Arbeitsgrundsaeetze.

1. Die Gemeinschaftsarbeit.

Die fruchtbarste Arbeitsform in der Entzifferung ist die Interessengemeinschaft einiger weniger, aufeinander abgestimmter E-Maenner, die sich insbesondere bei der Bearbeitung sehr schwieriger Probleme auch ohne Anordnung von oben instinktiv zusammenfinden und sich in ihrer geistigen Konstitution gegenseitig ergaenzen: Neben dem exakten, unerbittlich logischen und konstruktiven Systematiker mit vielleicht nur mittelmessigen Sprachkenntnissen steht der vorzuegliche Linguist aber ein wenig unbeholfene Kombinator, steht der sensible Kuenstler mit ausgesprochenem Fingerspitzengefuehl. Wenn der eine zu ermueden und zu verzweifeln beginnt, wird die gemeinsame Arbeit durch den Schwung der anderen trotzdem weitergetrieben. Diskussionen helfen ueber die Gedankenluecken des einzelnen hinweg, Oppositionen erhaerten richtige Erkenntnisse und bringen Verschaemendes und Gestuempertes zu Fall. Kurz, das Problem wird sozusagen "von allen Seiten ausgeleuchtet".

TOP SECRET

TOP SECRET

2. Die Raumfrage

Aus diesem Grunde schon ist die zuweilen laut werdende Forderung nach Separatraeumen als Idealfall, um angeblich Ruhe und geistige Konzentration zu garantieren, unsinnig. Notwendig dagegen ist eine gewisse Weitraeumigkeit der Arbeitsstaette. Die Raeume muessen so gross sein, dass die Bearbeiter sich nicht gegenseitig behindern, nicht aus Platzmangel grosse Spruch- und Unterlagenpyramiden entstehen, aus denen sich der Bearbeiter das im Augenblick Benoetigte muehevoll und unter grossen Zeitverlusten zusammensuchen muss. Insbesondere muss fuer zusaetzliche Sortiertische und ausreichende Ablagemoeglichkeiten gesorgt werden. Die disziplinierte Ruhe eines wissenschaftlichen Instituts muss im Interesse der Arbeit garantiert werden, wenn auch kurze und durchaus notwendige Arbeitspausen den ernsten Raum in eine froehliche Schwatzbude verwandeln.

3. Die Statistik.

Die Statistik, der Extrakt eines Chi-Spruches und seine chemische Analyse zugleich ist fuer den E-Mann das wesentlichste Hilfsmittel bei seinen Bemuehungen. Eine nachlaessig ausgefuehrte Statistik kann wertlos sein, zu Fehlschlussen fuehren und so den Gang der Bearbeitung stark versoenern.

Aus diesem Grunde ist die Bestellung von Hilfskraeften, die auf Grund ihrer Vorbildung und einer sehr geringen geistigen Eindringtiefe als "Nurstatistiker" zu gebrauchen waeren, aeusserst gefaehrlich und abzulehnen. Jeder E-Mann ist dazu anzuhalten, die fuer seine Arbeit notwendigen Hilfsstatistiken selbst zu erstellen. Eine Ausnahme bildet natuerlich die Bearbeitung sehr schwieriger und umfangreicher Verfahren, eine Wurmbearbeitung z.B., die wochenlange statistische und rechnerische Vorarbeiten voraussetzt.

TOP SECRET

TOP SECRET

4. Die Verantwortlichkeit des Bearbeiters.

Jeder Bearbeiter ist verpflichtet, seinen Spruch bis zur tatsächlichen Mitlesbarkeit verantwortlich zu bearbeiten und ihn abschliessend mit seinem Signum zu versehen, damit die Uebersetzer und Inhaltsauswerter, aber auch der Schichtfuhrer, ihre Rueckfragen jederzeit an den richtigen Mann wenden koennen. Die bearbeiteten Sprueche werden gesammelt und vom Schichtfuhrer oder einer besonders beauftragten Person fluechtig ueberprueft, und dann an die Inhaltsauswertung zum Uebersetzen weitergeleitet.

5. Die Spruchuebersetzung.

Solange nicht der Grossteil des Personals in der Inhalts- und Endauswertung ueber ausreichende Sprachkenntnisse verfuegt - und das war leider nur bei der Regimentsauswertung der Fall - maessen alle mitgelesenen Sprueche uebersetzt werden.

In der ersten Zeit wurde der Entzifferer angehalten, die von ihm bearbeiteten Sprueche selbst zu uebersetzen. Dieses Prinzip hat sich aber als hoechst unpraktisch erwiesen, denn ein betraechtlicher Teil des E-Personals verfuegte doch nicht ueber so gute Sprachkenntnisse, um die zum Teil verstuemelten und schwierigen Sprachtexte einwandfrei uebersetzen zu koennen.

In der Folge wurden mittelmaessige Entzifferer mit sehr guten Sprachkenntnissen zu einer besonderen Uebersetzergruppe zusammengefasst, die im Rahmen der Inhaltsauswertung das ganze mitgelesene Material bearbeiteten und sich zu guten Uebersetzungsspezialisten und gleichzeitig zu Hilfsauswertern entwickeln konnten. Darueber hinaus bildeten sie gewissermassen eine Kontrollstelle fuer die Arbeit der E-Abteilung.

TOP SECRET

TOP SECRET

6. Zum Personaleinsatz.

Jeder Entzifferer soll das Material und die Probleme bearbeiten, die er gerade noch- ohne grossere Zeitverluste natuerlich - bewaeltigen kann. Das schliesst aber nicht aus, dass auch vorzuegliche E-Maenner in der Zeit geistiger Erschoepfungszustaende stillschweigend leichte und primitive Arbeiten uebernehmen. In der Regel ist es aber angebracht, dass eine erstklassige Kraft ein Verfahren nicht bis zum Schluss bearbeitet, sondern nach dem Ausdemwegeraeumen aller Schwierigkeiten dieses Verfahren an schwaechere Kameraden abgibt und so wieder fuer Schwieriges zur Verfuegung steht.

7. Die Allgemeinverstaendlichkeit der persoenlichen Unterlagen.

Bei der Bearbeitung eines Verfahrens muessen alle wesentlichen Zwischenkenntnisse schriftlich niedergelegt werden, und zwar so verstaendlich, dass bei unvorhergesehenem Ausfall des Bearbeiters ein anderer die Arbeit ohne Zeitverlust aufnehmen kann. Schon aus diesem Grunde allein werden fuer verschiedene Arbeitsvorgaenge (z.B. Abfassung von Statistiken, Erstellung von Ueberschliessungssystemen) allgemein gueltige Normen und schriftliche Symbole eingefuehrt, die die Allgemeinverstaendlichkeit aller persoenlichen Unterlagen fuer den gesamten Mitarbeiterkreis garantieren.

8. Einsatz weiblicher Arbeitskraefte.

Waehrend der Mann um der Sache willen arbeitet, arbeitet die Frau mehr um der Person willen. Ihre Arbeitsleistung ist also viel mehr als beim Mann von ausgelosten Sympathie- oder Antipathie-Impulsen abhaengig. Die Arbeitsleistung war also sehr stark von der Haltung des Chefentzifferers, der sonstigen militaerischen Vorgesetzten und der allgemeinen Lebensbedingungen abhaengig.

TOP SECRET

TOP SECRET

Wenngleich eine ganze Anzahl von intelligenten Frauen und Maedchen gute Durchschnittsleistungen gezeigt haben, wurde doch durch das Zusammenarbeiten und meist auch durch das enge Zusammenleben in kriegsbedingten Verhaeltnissen eine Atmosphaere erzeugt, die nicht gerade wissenschaftlich und ernst zu nennen gewesen ist. Zweifellos haben reine Maenner-Besatzungen bessere und solidere Arbeitsleistungen aufgewiesen.

9. Militaerischer oder ziviler Einsatz?

Alle E-Fachleute sind der Meinung, dass ein ziviler Einsatz sich auf die Arbeitserfolge der Entzifferung bestimmt positiv ausgewirkt haette. Durch die herrschende militaerische Lebensform wurde ein Teil der persoenlichen Arbeitsenergien auf fuer die Arbeit vollkommen abwegige Gebiete abgeleitet. So hat z.B. der militaerische Ausbildungsdienst wertvolle Arbeitsstunden in Anspruch genommen, die Masse des E-Personals aber doch nicht zu wirklich gut ausgebildeten Soldaten gemacht. Leider waren auch die Widerstaende bei der Einreichung von Befoerderungsvorschlaegen fuer verdiente Entzifferer immer wieder recht gross. Die zustaendigen militaerischen Vorgesetzten haben sich immer wieder - und nicht ganz mit Unrecht - gestraebt, die Vorgeschlagenen zu befoerdern, weil sowohl ihre soldatische Haltung als auch der Ausbildungsstand tatsaechlich viel zu wuenschen uebrig liess. So war es aber nicht immer moeglich, verdiente Entzifferer fuer ihre hervorragenden Arbeitsleistungen entsprechend zu belohnen.

F. Die Hilfsmittel des Entzifferers

1. Allgemeine Hilfsmittel

Bei der staendigen Entwicklung der Militaersprache stoesst auch der gute Sprachler taeglich auf unbekannte Woerter, Ausdruecke und Abkuerzungen. In diesem Falle leisten Fachwoerterbuecher, Abkuerzungsverzeichnisse und ganz allgemein

TOP SECRET

TOP SECRET

gesehen auch fachliche Ausbildungsbuecher des Gegners gute Dienste. Da aber die Redaktion derartiger Spezialarbeitsbehelfe meist laengere Zeit in Anspruch nimmt, ist der E-Mann genoetigt, sich selbst zu helfen: Laufend auftauchende sprachliche Fragen und Unklarheiten werden schriftlich festgehalten und bei der naechsten Gelegenheit geklaert (Vernehmung besonders intelligenter Gefangener). Der Vernehmungsoffizier der Luftflotte wird dauernd in Anspruch genommen, soweit nicht noch guenstigere lokale Moeglichkeiten (Gefangenenlager in der Naehel) ein selbstaendiges Vorgehenszweckentsprechender erscheinen lassen.

Netzbilder, Rufzeichendeutungen und Feilerggebnisse werden zur Identifizierung des Chi-Materials nicht nur von der Registratur, sondern auch von einzelnen Bearbeiter gebraucht.

Karten, Ortsverzeichnisse und Kursbuecher erleichtern den Einbruch und die Ausarbeitung des Materials. Zu denselben Zwecken werden Dislokationskarten und Verzeichnisse, Flugzeugtafeln, Typenverzeichnisse aller Art, Truppen- und Namenkarteien benutzt.

2. Spezielle Hilfsmittel

a) Die Sprachstatistik

Bei der langjaehrigen Bearbeitung eines Landes treten die klassischen Sprachstatistiken (Buchstaben-, Bigramm-, Trigrammstatistik usw.) vollkommen in den Hintergrund. Die wenigen, noch gebrauchten Faustregeln werden zum allgemeinen Gedankengut.

b) Das Brueckenverzeichnis.

Neulinge und sprachlich unsichere Mitarbeiter haben zum Teil selbst angefertigte sogenannte "Brueckenverzeichnisse", in denen markante Sprachtexte

TOP SECRET

TOP SECRET

analysiert sind, gebraucht. Zuweilen haben diese "Bruecken" gute Dienste geleistet, werden aber von den erfahrenen E-Maennern meistens abgelehnt.

c) Das Idealsatzbuch.

Die Zusammenfassung des Sprachschatzes aus der Fuelle der konstruierten und den wenigen Beutesatzbuechern zu einem Satzbuchextrakt, zu einem Idealsatzbuch gewissermassen, hat sich insbesondere bei Ausarbeitungen gut bewahrt. Solche Idealsatzbuecher sind waehrend des Krieges mehrfach herausgegeben worden.

d) Das Statistikformular.

Im Laufe der Jahre sind an die 20 verschiedene Statistikformulare entwickelt worden, von denen die meisten fuer die laufenden Bearbeitungen gebraucht worden sind.

e) Das Sprucharchiv.

Das Archiv alter mitgelesener Sprueche ist bei der Bearbeitung neuer Verfahren bei bekannten Netzen und bei der Weiterbildung des E-Personals als Anschauungsmaterial von grossem Wert.

Taegliche Aufzeichnungen in Form von Heften bzw. Karteien ueber das Auftreten einzelner Verfahren, ueber die Beziehung zwischen Verfahren einerseits und Rufzeichen, An- und Unterschriftsgruppen, Ortsnamen, Signalgruppen, charakteristischen Spruchkoeffen und charakteristischem Spruchaufbau andererseits vervollstaendigen die Reihe der Hilfsmittel fuer den Entzifferer.

3. Die Beuteauswertung

Waehrend der deutsche Heeres-N-Dienst bei den Vormarschen im Osten sehr viel Schluesselunterlagen erbeutet hat, ist der Beuteanfall bei der Luftwaffe, schon infolge der grosseren Frontferne, kaum ins Gewicht gefallen, so dass bei

TOP SECRET

TOP SECRET

der Arbeit eine fühlbare Entlastung nicht zu verzeichnen gewesen ist. Ein Gross-
teil der anfallenden Beute war entweder stark veraltet (so sind z.B. in den ersten
Tagen des Ostkrieges Schlüsselmittel aus dem Jahre 1935 angefallen) oder wegen
der erkannten Kompromittierung nicht mehr im Gebrauch. Boden-Bord-Tafeln aus ab-
geschossenen Maschinen konnten wegen der kurzen Anwendungsdauer dieser Tafeln
(meist nur ein Feindflug) ebenfalls sehr selten ausgewertet werden.

Die Weiterleitung erbeuteter Fliegerschlüssel ueber H-Einheiten des
Heeres und die H-Verbindungsoffiziere (HVO) bei den Flottenstaeben und sonstigen
fliegenden Verbaenden war im allgemeinen garantiert.

Manchmal waren auch Beutebefehle mit Ueberschlüsselungsangaben von
im Gebrauch befindlichen Verfahren von grossem Wert gewesen, da sie wertvolle
Rueckschluesse auf den Aufbau des Verfahrens zuliessen.

G. Die Zusammenarbeit der E-Abteilung mit anderen Fachinstitutionen

1. Die Zusammenarbeit mit den anderen Abteilungen der Auswerte-Kompanie

a) Die Zusammenarbeit mit dem Funker

Eine enge Verbindung zwischen Funker und Entzifferer hat sich stets
als sehr fruchtbar erwiesen. Haeufige Ruecksprachen geben dem Entzifferer fuer
seine Arbeit wertvolle Hinweise. Das Wissen um die Qualitaet des einzelnen Funkers
um seine arbeitsmaessigen Vorzuege aber auch um seine charakteristischen Fehler, er-
spart dem E-Mann manchen Irr- und Umweg. Gerade bei Neuentzifferungen ist es aus-
serst wichtig, das vorliegende Material nach der Qualitaet der aufnehmenden Funker
bewerten zu koennen.

Gelegentliche allgemein gehaltene Vortraege des Chefentzifferers
vor den Funkern ueber die Entzifferung und den Wert eines einwandfreien Sprachmater-
ials haben auf den Dienstleister der Funkschichten sehr positiv gewirkt.

TOP SECRET

TOP SECRET

b) Peil- und Betriebsauswertung.

Die Sprueche werden vor ihrer Bearbeitung in der E-Abteilung in der Betriebsauswertung durchgearbeitet und ausgemerkt. Eine Aussprache mit dem Betriebsauswerter kann dem E-Mann fuer den Einzelfall wertvolle Anregungen geben.

Andererseits ist aber auch der Entzifferer in der Lage, der Betriebsauswertung verlorengegangene Netze durch Spruchidentifizierungen auf Grund von Signal- und Kenngruppen und markanten Statistiken wieder heranzuholen.

In gewissen Faellen koennen - insbesondere bei spaerlichen Erkenntnissen der Betriebsauswertung - auch Peilerggebnisse von beachtlicher Wichtigkeit sein.

c) Inhalts- und Endauswertung

Alle Karteien und sonstigen Unterlagen der Auswertung koennen von der E-Abteilung fuer ihre Arbeit laufend herangezogen werden. Es hat sich sogar immer wieder bewahrt, dass bei der Bearbeitung schwieriger Probleme sich E-Maenner und Auswerter zusammensetzen, gewissermassen zusammen entziffern.

Die taeglichen Arbeitsbesprechungen unter dem Vorsitz des Kommandeurs bzw. des Ia der Abteilung gaben auch dem Chefentzifferer die Moeglichkeit, Wuensche und Anregungen fuer die Zusammenarbeit vorzubringen.

Oberster Grundsatz aller Zusammenarbeit ist die Erkenntnis, dass jede Fachabteilung die anderen fuer ihre Arbeit braucht und auch selbst gebraucht wird, dass jede Fachrichtung gewissermassen die Hilfswissenschaft fuer die anderen darstellt, dass die einzelne Abteilung fuer sich allein nie erfolgreich arbeiten koennte.

TOP SECRET

TOP SECRET

Zu Beginn des Krieges hat es Bestrebungen gegeben, die einzelnen Fachabteilungen aus Geheimhaltungsgründen voneinander abzukapseln und einen Gedankenaustausch zu unterbinden; dieser unsinnige Gedanke wurde in kuerzester Zeit wieder fallen gelassen.

2. Die Zusammenarbeit der E-Abteilung mit anderen Entzifferungsstellen

a) Regimentsentsifferung (frueher Referat E 1)

Urspruenglich war der Kontakt zwischen Regiment und Abteilung auf dem Gebiete der Entzifferung sehr eng, weil die Abteilungen weder personell noch materiell den gestellten Anforderungen nachkommen konnten. Haeufige Kommandierungen und Arbeitsbesprechungen gewahrleisteten die Vermittlung neuer Erkenntnisse und Arbeitsmethoden.

Infolge der Differenzierung des Chi-Materials, der zum Teil sehr grossen Entfernungen im Osten und der schlechten Nachrichtenverbindungen wurde der Kontakt im Laufe der Zeit allerdings lockerer. Die Abteilungen waren spaeter in der Lage, ihr Aufgabengebiet vollkommen selbstaendig zu bearbeiten (bis auf 5-Z).

Neue Verfahren wurden mit dem Regiment staendig auf dem Fernschreibwege ausgetauscht, ihre Nummerierung erfolgte durch das Regiment. - Ausnahmsweise konnte fuer den Nachrichtenaustausch der E-Abteilungen der Funkstern des H-Dienstes im Osten benutzt werden. Fuer die Funksprueche der Entzifferung stand ein besonderes Schluesselverfahren zur Verfuegung. Es ist erwachnenswert, dass diesem Verfahren zeitweise ein sowjetisches Satzbuch zugrunde gelegen hat.

Vierteljaehrliche Arbeitsbesprechungen von mehrtaegiger Dauer gaben den Chefentzifferern der Abteilungen die Moeglichkeit, alle anfallenden fachlichen und organisatorischen Fragen beim Regiment zu klaeren.

TOP SECRET

TOP SECRET

b) Nachbarabteilungen des Regiments:

Die drei E-Abteilungen an der Ostfront standen im lebhaften Gedankenaustausch. Häufige gegenseitige Besuche gewährten Einblick in die Arbeit der Nachbarabteilungen und gaben neue Anregungen fuer die eigene Arbeit. Neugelesene Verfahren der gemeinsam beobachteten Naht-Luftarmeen wurden auf dem Fernschreibwege direkt ausgetauscht, die Unterlagen fuer aeltere und ausgearbeitete Verfahren in gewissen Zeitabstaenden verglichen. Die Tatsache, dass die Spitzenkraefte bei allen E-Abteilungen entweder aus der Chi-Stelle hervorgegangen sind oder sonst irgendwo zum Teil jahrelang zusammengearbeitet haben und sich gut kannten, fuehrte zu einer sehr erspriesslichen und loyalen Zusammenarbeit.

c) E-Gruppen bei abgesetzten Kompanien der H-Abteilung.

Das Personal dieser E-Gruppen war in den meisten Faellen aus der E-Abteilung herausgezogen, es wurde auch in der Folgezeit laufend von der E-Abteilung der Auswerte-Kompanie betreut und blieb arbeitsmaessig an sie stark angelehnt.

d) Die Zusammenarbeit mit anderen Wehrmachtteilen und auslaendischen H-Diensten

Wenngleich das Arbeitsgebiet der einzelnen E-Abtlg. auf Grund der Eigenart der sowjetischen Schluesselmethoden fest umrissen gewesen ist, wurde der laufende Meinungs-austausch mit den entsprechenden Fachstellen anderer Wehrmachtteile und befreundeter auslaendischer H-Dienste angestrebt und fuehrte zu guten Ergebnissen und zu einer Erweiterung des fachlichen Horizonts.

a) Die Zusammenarbeit mit dem Heer.

Die Zusammenarbeit mit den E-Abteilungen der im selben Raum liegenden "Kommandeure der Nachrichtenaufklaerung" (NA) war durchweg gut. Es

TOP SECRET

TOP SECRET

wurde sogar immer wieder ein regelrechter Materialaustausch zwischen den einzelnen E-Abteilungen von Heer und Luftwaffe vereinbart. Er kam aber nie richtig zum Tragen, weil das gegenseitige Interesse an den einzelnen Verfahren doch nicht so gross gewesen ist. Aber das Charakteristische der Verfahren, die sich daraus ergebenden Entzifferungsmethoden und die allgemeine Arbeitsorganisation wurde immer wieder besprochen bzw. besichtigt. Ausserdem wurde das interessierende Spruchmaterial laufend ausgetauscht.

Im Gegensatz zur Luftwaffe verfuegten die Heeresstellen ueber eine grosse Tradition, die teilweise allerdings in eine geistige Unbeweglichkeit auszuarten drohte und die Organisation der Arbeit schwerfaellig erscheinen liess. Die Arbeitserfolge des Heeres sind im Laufe des Krieges infolge der laufenden Komplizierung der Heeresverfahren und einer sehr strengen Funkdisziplin der Sowjets kleiner geworden. Arbeitsmethoden und Ausbildungsstand waren im Grosse, Ganzen im Vergleich zur Luftwaffe annaehernnd gleich.

b) Die Kriegsmarine.

Die Zusammenarbeit mit der Marine war nicht so eng, was in erster Linie auf das Auseinandergehen der tatsaechlichen Fachinteressen zurueckzufuehren gewesen ist. Im uebrigen gilt im wesentlichen das unter a) Aufgefuehrte.

c) Waffen-SS

Eine Zusammenarbeit bestand nicht. Gespraechsweise war von der Existenz einer grosszuegig aufgebauten Entzifferung der SS die Rede. Vereinzelt wurde der Versuch unternommen, Spitzenfachkraefte der anderen Wehrmachtteile fuer die SS zu gewinnen.

TOP SECRET

TOP SECRET

d) Der finnische H-Dienst

Die finnische Entzifferung war straff und zweckmässig in einer grossen Zentralstelle organisiert, verfügte ueber eine Vielzahl von vortrefflichen Kraefte und hatte dementsprechend grosse Erfolge.

Die Zusammenarbeit mit der E-Abteilung bei der Luftflotte 1 war vorbehaltlos und fuhrte zu ausgezeichneten Ergebnissen.

e) Der ungarische H-Dienst

Der Entzifferungsapparat der Ungarn war personell ueberaltert und sehr unbeweglich, die Arbeitsergebnisse waren dauerhaft. Obwohl bereits vor dem Kriege eine getarnte Luftwaffendienststelle in Budapest (W.s.b.V.) mit den Ungarn zusammenarbeitete, konnte das Verhaeltnis nie als zufriedenstellend bezeichnet werden, weil die Ungarn es an der notwendigen Ehrlichkeit fehlen liessen.

V. DER ENTZIFFERER

A. Geistige Voraussetzungen

Allererste Voraussetzung ist ein waches Interesse an der Arbeit. Wer nicht will, an der Arbeit nicht interessiert ist, kann nicht zu irgendwelchen Leistungen gezwungen werden. In diesem Falle stellt er nur einen leistungsfreudigen Fremdkoerper dar.

Der E-Mann muss intelligent und geistig sehr beweglich sein, doch muss der kombinatorische Ideenreichtum durch eine ausgesprochene kritische Haltung in Schach gehalten werden. Fantasten sind als Entzifferer nicht denkbar.

Das Vermoegen, wissenschaftlich, d.h. systematisch arbeiten zu koennen, ist eine weitere wesentliche Voraussetzung. Die Eigenart des Berufes bringt es nur all zu haeufig mit sich, dass die Arbeit von Tagen ja von Wochen sich als

TOP SECRET

TOP SECRET

zwecklos herausgestellt, dass immer wieder neue Wege beschritten werden müssen, um das gesteckte Ziel zu erreichen; in diesem Falle hilft nur eine unentwegte Zähigkeit.

Gute Sprachkenntnisse sind unerlässlich. Liegen aber keine zufriedenstellenden Sprachkenntnisse vor, so muss zumindest ein ausgesprochenes Sprachgefühl gefordert werden.

Die so oft verlangte oder vorausgesetzte mathematische Begabung gehört tatsächlich dazu, doch darf diese Begabung nicht mit einer mathematischen Schulbildung verwechselt werden. Die besten E-Männer mit grossen analytischen und konstruktiven Fähigkeiten haben in der Regel von den Lehrsätzen der Kombinatorik keine Ahnung. Die wenigen mathematisch gebildeten Mitarbeiter dagegen besitzen ihre Kenntnisse oft lediglich dazu, anhand geläufiger Formeln auszurechnen, wieviel Möglichkeiten dieses oder jenes Verfahren zulässt - entziffert aber werden diese Verfahren meist von anderen.

Nicht zu vergessen sind noch zwei Elemente: Fingerspitzengefühl und -Glück. Gemeint ist das Glück, das auf die Dauer allerdings nur dem Tüchtigen beschieden ist.

Diese Ausführungen deuten zur Genüge an, dass auf Grund der gestellten Forderungen das berufliche Idealbild nur von sehr wenigen erreicht werden kann. Deshalb schon muss im Interesse der Arbeit der Einzelne ein ausgesprochenes Gemeinschaftsgefühl besitzen, er darf kein Einzelgänger sein.

Die meisten Erfolge der Entzifferung sind nicht das ausschliessliche Werk eines Einzelnen, sondern Gemeinschaftsleistungen, die aus der fachlichen

TOP SECRET

TOP SECRET

Diskussion, aus der gegenseitigen Kritik, aus einer Integration von Fingerspitzengefühl, Systematik und Emsigkeit entstanden sind.

Es gibt keinen Entzifferer mit fachlichen Universalkenntnissen. Und zwar liegt dieses weniger an der geistigen Eindringtiefe des E-Mannes als an den Erfindern der bearbeiteten Schlusself Verfahren und an dem zufaelligen, meist auf Grund der Sprachkenntnisse gelenkten Einsatz des einzelnen. Jeder beherrscht nur die Verfahren und die zur Loosung dieser Verfahren benoestigten Kunstgriffe, die er tatsaechlich bearbeitet hat, und zwar nicht kurzfristig - vielleicht auf irgendeiner Schule oder auf einem Lehrgang, - sondern waehrend einer mehr oder weniger langen Zeitperiode in der Praxis. Ein hervorragender E-Mann, der jahrelang nur die Ersatzverfahren einer bestimmten Laendergruppe etwa bearbeitet hat, wird ueber Maschinenverfahren nur ganz Allgemeines aussagen koennen, woenngleich angenommen werden muss, dass er auf Grund seiner bewiesenen fachlichen Begabung auch auf diesem Gebiet seinen Mann wird stehen koennen.

B. Die Auswahl des E-Personals

Durch die strikte Forderung nach Geheimhaltung werden Auswahl bzw. Ersatz des Personals stark erschwert. Spezielle psychotechnische Pruefungen sind begreiflicherweise verfaenglich, allgemeine Intelligenspruefungen fuehren immer wieder zu argen Misagriffen. Nach jahrelanger Erfahrung auf dem Gebiete der Personalauswahl muss man zu der Ueberzeugung kommen, dass ein allgemeines Gespraech von 10 Minuten Dauer die Eignung oder Nichteignung eines Anwaerter besser erkennen laesst, als alle langwierigen und umfangreichen Pruefungen. Natuerlich, gelegentliche Fehlurteile lassen sich nie ganz vermeiden. Manch hoffnungsfreudiger Neuling entpuppt sich schon nach einigen Wochen als unbegabter Stueemper und manch unscheinbarer Mensch mit offensichtlich grossen Manki (ungeruegende Sprachkenntnisse, mangelhafte Allgemeinbildung usw.) wird ein erfolgreicher und qualifizierter Entzifferer.

TOP SECRET

TOP SECRET

So hat z.B. ein zweifellos sehr intelligenter Sprachlehrer, der etliche anerkannt gute Lehrbuecher der russischen Sprache verfasst hat, als Entzifferer vollkommen versagt. Auf der anderen Seite ist ein ganz zufaellig zum H-Dienst gekommener junger Soldat, Metallarbeiter von Beruf, der nie zuvor wissenschaftlich gearbeitet hatte, einer der erfolgreichsten Entzifferer geworden.

Ein fuer Arbeitsfreudigkeit und Arbeitsleistung nicht zu unterschaeztender Faktor war die Tatsache, dass zahlreiche E-Maenner Russland-, Baltendeutsche und auch nationalrussische Emigranten gewesen sind, die alle persoenlich ihre sehr ueblen Erfahrungen mit dem Bolschewismus gemacht hatten. Fuer diese Menschen war die Beschaeftigung in der Entzifferung nicht allein Broterwerb bzw. befohlener Dienst sondern auch der Ausdruck einer starken antibolschewistischen Gesinnung.

In den letzten Kriegsjahren wurde der Ersatz fast ausschliesslich von der Dolmetscher Ersatz-Abteilung der Luftw. gestellt. Es hatte sich bitter geraecht, dass sich bei dieser Abteilung kein Ausbilder mit E-Fachkenntnissen befunden hatte der die fuer einen E-Einsatz in Frage kommenden Maenner haette auswahlen koennen. So entsprach der zur Verfuegung gestellte Ersatz keinesfalls den gestellten Anforderungen.

C. Die Ausbildung des E-Personals.

1. Die laufende Ausbildung

Ein Entzifferer bildet sich fast ausschliesslich durch die laufende praktische Arbeit einer E-Abteilung.

Zuerst ist der Neuling der Lehrling eines erfahrenen Entzifferers. Allerdings, es wird nicht alles an ihn herangetragen werden koennen, er muss sich jede Neuheit, jeden Kniff und Kunstgriff erfragen und - erarbeiten. Denn mit

TOP SECRET

TOP SECRET

der Erklarung allein ist es ja nicht getan. Die Erklarung z.B., wie man eine Ueberschlusselung loest oder wie man eine Relativunterlage an das vermutliche Original angleicht, versetzt ihn noch lange nicht in die Lage, diese Arbeitsgaenge tatsaechlich selbstaendig auszufuehren. Vermag der Neuling nicht das Problematische seiner Arbeit selbst zu sehen, verspuert er nicht selbst den Wunsch, durch staendig Fragen und Bohren einen Einbruch in dieses Neuland zu erzwingen, wird er auch nie ein guter E-Mann werden. Versager des Berufes entschuldigen sich wohl haeufig damit, man haette ihnen irgend etwas nicht gezeigt oder nicht erklaert. Es ist dann wohl immer so, dass sie nicht die notwendige geistige Eindringtiefe besessen haben, um sich das entsprechende Problem selbst zu erarbeiten. Denn: Gezeigt wird grundsaeztlich alles, es muss aber auch verstanden werden.

Junge Mitarbeiter sind aber selbstverstaendlich keine geistigen Laufjungen, deren Arbeitszeit ausschliesslich mit Spruchsortiment und Statistizierungen deren Sinn ihnen wohlmoeglich nicht erklaert wird, ausgefuellt werden soll. Zu Beginn einer langen und muhevollen Ausbildung muss man gerade den Neuling am aufregenden, ja dramatischen Geschehen dieser Arbeit teilnehmen lassen, ihm etwa einen Durchbruch oder die systematische Entwicklung einer Bearbeitung aufzuzeigen versuchen.

Daneben ist der grosste Wert darauf zu legen, dass der junge Entzifferer es lernt, die mannigfaltigen Hilfsmittel all der anderen Abteilungen bei seiner eigenen Arbeit sinnvoll und zweckmaessig zu verwenden, denn der beste Entzifferer ist nicht derjenige, der auf sich allein gestellt und voraussetzungslos arbeitet, sondern der sich moeglichst viele Bausteine fuer seine Kombinationen und Konstruktionen aus den Arbeitsergebnissen der anderen Abteilungen zusammensucht. Ueberspitzt ausgedrueckt besteht die Kunst nicht darin, moeglichst viel "schoepferisch" zu arbeiten, sondern moeglichst viele bekannte und mechanische Elemente in seinen Arbeitsprozess aufzunehmen.

TOP SECRET

Aus diesem Grunde ist es unumgaenglich, dass der Entzifferer auch taktisch geschult wird und die Arbeit der einzelnen Auswerteabteilungen zumindest in groben Umrissen kennt. Mit Grausen muss der zahlreichen Mitarbeiter der ersten Jahre gedacht werden, die infolge Fehlens auch der primitivsten militaerischen Kenntnisse sich nicht scheuten, in ihren bearbeiteten Spruechen Divisionsstaebes Regimentern zu unterstellen und von ihnen Befehle empfangen zu lassen oder Nahaufklaerer zum Fernkampfeinsatz starten zu lassen usw. und bei den berechtigten Beanstandungen ihrer Arbeit zu behaupten, ihre Gedankengaenge und Unterlagen stimmten, und bei unbefriedigendem Text waere es eben unaso schlimmer fuer den Text.

Ein Grundzug des auch recht guten E-Mannes ist sein Hang zum Konservatismus, der Hang zum Festhalten an Arbeitsmethoden, die sich einmal "auch" bewahrt haben. Es ist sehr schwer, Mitarbeiter davon zu ueberzeugen, dass ihre bis jetzt angewandten Methoden zwar auch zum Ziel gefuehrt, aber durch noch bessere, noch logischere und noch exaktere ersetzt werden koennen bzw. muessen. In diesen Augenblicken macht sich stets eine gewisse geistige Traegheit bemerkbar. Die Einfuehrung der Arbeit nach Tauschtafeln z.B. oder die Verankerung der Idee, dass es unbedingt notwendig ist, den Versuch zur tatsaechlichen Rekonstruktion der Originalunterlage auch dann zu unternehmen, wenn die Arbeit nach einer Relativunterlage auch erfolgreich gewesen ist, verlangt von verantwortlichen Entzifferer viel Zeit, Kuehe und paedagogische Ueberredungskunst.

2. Der Lehrgang.

Der Mangel an gutem E-Personal was leider so empfindlich, dass es nicht moeglich gewesen ist, einige gute Maenner aus der taeglichen Arbeit herauszuloesen zum Zwecke der Aufstellung eines permanenten Lehrstabes und zur Durchfuehrung langfristiger Ausbildungslehrgaenge.

TOP SECRET

TOP SECRET

Alle durchgefuehrten kurzfristigen und letzten Endes improvisierten Entzifferungs-Lehrgaenge aber haben immer wieder ihre Unzulaenglichkeit und Fragwuerdigkeit erwiesen. In wesentlichen konnten ja nur Verfahren kurz durchgesprochen und die Beschaffenheit der zur Bearbeitung dieser Verfahren notwendigen Hilfsmittel aufgezeigt werden. Jede konstruierte Uebungsaufgabe ist ja einmalig und erzieht mehr zum Formalismus als zur notwendigen Wendigkeit. Das war auch alles - d.h. sehr wenig.

So sind kurzfristige Lehrgaenge meist nur die Staetten zum Kennenlernen neuer Mitarbeiter. Das Produkt dieser Lehrgaenge ist aber nie der "ausgebildete Entzifferer". Der bildet sich, wie bereits ausgefuehrt, ausschliesslich in der Praxis und durch die Praxis.

3. Das Lehrbuch.

Zweifellos waere es aber richtig gewesen, aus dem Erlebnis der Praxis heraus die Grundgedanken und Kunstgriffe der Entzifferung in Form eines Leitfadens schriftlich niederzulegen und nicht nur dem Neuling sondern auch dem Fortgeschrittenen als Lehrbuch bzw. Nachschlagewerk an die Hand zu geben.

Der Vorschlag zur Durchfuehrung dieser Arbeit sollte nach dem Kriege verwirklicht werden.

TOP SECRET